Optimal Data Compression for Lifetime Maximization in Wireless Sensor Networks Operating in Stealth Mode

Davut Incebacak[a], Ruken Zilan[b], Bulent Tavli[c], Jose M. Barcelo-Ordinas[b,*], Jorge Garcia-Vidal[b]

[a]*Middle East Technical University, Ankara, Turkey*
[b]*Universitat Politecnica de Catalunya-BarcelonaTECH (UPC), Spain*
[c]*TOBB University of Economics and Technology, Ankara, Turkey*

Abstract

Contextual privacy in Wireless Sensor Networks (WSNs) is concerned with protecting contextual information such as whether, when, and where the data is collected. In this context, hiding the existence of a WSN from adversaries is a desirable feature. One way to mitigate the sensor nodes' detectability is by limiting the transmission power of the nodes (*i.e.*, the network is operating in the stealth mode) so that adversaries cannot detect the existence of the WSN unless they are within the sensing range of the WSN. Position dependent transmission power adjustment enables the network to maintain its level of stealth while allowing nodes farther from the network boundary to use higher transmission power levels. To mitigate the uneven energy dissipation characteristic, nodes that cannot dissipate their energies on communications reduce the amount of data they generate through computation so that the relay nodes convey less data. Dynamic data compression/decompression strategies reduce the amount of data to be communicated, thus, they achieve better energy savings when compared to static compression/decompression of data in which the data is always compressed independently of the power transmission strategy. In this study, we investigate various data compression strategies to maximize the lifetime of WSNs employing contextual privacy measures through a novel Mathematical Programming framework.

Keywords: Wireless Sensor Networks, Contextual Privacy, Data Compression, Network Lifetime

*Corresponding author.
Email addresses: idavut@metu.edu.tr (Davut Incebacak), rzilan@ac.upc.edu (Ruken Zilan), btavli@etu.edu.tr (Bulent Tavli), joseb@ac.upc.edu (Jose M. Barcelo-Ordinas), jorge@ac.upc.edu (Jorge Garcia-Vidal)

1. Introduction

Wireless Sensor Networks (WSNs) are comprised of a plurality of low cost, limited power, and tiny sensor nodes. In WSN applications such as surveillance, physical measurements are taken by the sensors and reported to the sink node. One of the concerns in the design of a WSN is privacy preservation. Privacy enabling techniques are focussed with two main issues: data-privacy and contextual privacy. *Data-privacy* oriented techniques address the problem of preserving the privacy of the data collected by the sensors. On the other hand, adversaries are also interested in extracting contextual information (*e.g.*, which wireless sensor node has detected the object of interest?). *Contextual Privacy* focus on hiding the identity and location of the nodes, hiding traffic flows, and rendering the task of contextual information extraction more challenging (*i.e.*, defense-in-depth).

Under this scenario, many mechanisms that appear in the literature, [1, 2], propose the introduction of redundant traffic or extra transmissions. Lowering the transmission power avoids the introduction of these extra transmissions, but still remains the issue of reducing the energy consumption and balancing the load to evenly distribute the energy dissipation. Tavli et al. [3], introduced a Linear Programming (LP) framework for studying the tradeoffs in network lifetime and load balancing in contextual privacy scenarios under uniform sensor node deployments.

Data compression has widely been used to reduce the amount of traffic sent in a WSN, thus, to reduce the energy consumption. Yu et al. [4] proposed the concept of tunable compression that is able to adjust the computational complexity of lossless data compression based on the energy availability. The concept comes from compression tools such as gzip in which there are ten different levels of compression ratios. Since data compression and decompression in the nodes also dissipate energy, it is important to determine the energy savings achieved by different compression strategies.

There is a clear trade-off in the energy consumed by compressing/decompressing data and the savings obtained by sending less amount of data to next-hop nodes. Lowering the transmission power minimize the domain in which attackers may lie, however, such a contextual privacy preservation approach also renders some links inoperable that can be used to balance the energy dissipation throughout the WSN. Hence, the inter play among data compression/decompression, load balancing, and the extent of the vulnerable domain (*i.e.*, the area where adversaries may lie outside the sensing domain) is explored in this paper.

This paper is a substantially improved and expanded version of an earlier conference paper [5], where we investigated the effects of several data compression strategies on WSN lifetime while providing stealth mode of operation through an LP framework. In fact, the LP framework in [5] is obtained by integrating the LP

frameworks presented in [3] and [6]. Nevertheless, the main contribution of this study is the consideration of more practical aspects of data compression in WSNs providing contextual privacy against adversaries. More precisely stated, this paper extends the concept introduced in [5] by investigating the effects of Optimal Single Level Compression (OSLC) and Limited Compression (LC) strategies through Mixed Integer Programming (MIP) models. Furthermore, we explore the impact of node density and limited transmission range due to contextual privacy scenarios.

The rest of the paper is organized as follows. An overview of the related work is presented in Section 2. We construct and describe the mathematical programming framework in Section 3. Numerical analysis to explore the parameter space and to compare the performances of the proposed strategies are given in Section 4. Conclusions are given in Section 5.

2. Related Work

Privacy preservation in the context of WSNs has been surveyed in [1, 2]. Li et al. [1] focus their survey on data-oriented and context-oriented privacy while Conti et al. [2] focus their survey on context-oriented privacy techniques, more precisely, on Source Location Privacy (SLP) which is a term to express security measures for hiding the location of the source nodes. The authors classify adversaries having a partial view of the network as local adversaries while those ones having a total view of the network as global adversaries. An example solution against global attackers is the use of Network Coding [7] which have the disadvantage of increasing complexity in the sensing nodes. Most of the solutions proposed defend the network against local adversaries using techniques such as random walk [8], cyclic entrapment [9], delaying the packet [10] or limiting node detectability [3, 11]. Some other techniques are able to defend the network against local or global adversaries utilizing implementation dependent approaches (*e.g.*, use of dummy packets [8]).

As discussed earlier, our work can be classified within the limiting node detectability solutions proposed against local adversaries. Another prominent study in this class is by Dutta et al. [11] where it is considered that the attackers measure raw physical properties of messages like angle of arrival or the signal strength of the detected signal. In order to defend against this kind of attackers, they propose anti-localization by silencing in which sensors intelligently predict their own importance as a measure of two conflicting requirements: *localize the adversary* and *hide from the adversary*. Only some sensors will participate in message exchanges reducing the probability that the adversary detects events.

Our work deals with the hypothesis that local attackers want to be undetected while they observe the network. By limiting the transmission power of the nodes,

node detectability is restricted to a limited area outside the sensing area. In general, as Cheng et al. [12] show, limiting the transmission power implies the use of non-optimal routing paths with respect using the maximum transmission ranges, impacting, thus, the network lifetime. Tavli et al, [3], analyze the lifetime bounds improving contextual privacy by transmission range control. The authors show that maximizing the network lifetime increases the unobservability area in which the attacker can be placed, while decreasing the transmission range, network lifetime is reduced but the unobservability area is also reduced.

Data compression allows reducing the amount of data to be sent to the sink. In general, compression ratios and time complexity are the metrics used by compression algorithms to evaluate the performance of the mechanisms. Srisooksai et al. [13], survey data compression mechanisms in WSN. The authors classify data compression mechanisms into two broad classes: *distributed data compression* and *local data compression*. Distributed data compression approaches such as Distributed Source modeling (DSM), Distributed Transform Coding (DTC), Distributed Source Coding (DSC) and Compressed Sensing (CS) techniques are, typically, employed in dense sensor deployment cases. In our paper, we consider local data compression techniques that usually exploit temporal correlation of the data and do not depend on the specific WSN topologies. These techniques are classically categorized as lossless and lossy compression schemes. Examples of lossless compression are the well known LZW (Lempel-Ziv-Welch) algorithm and the simple lossless entropy compression (LEC) scheme proposed for WSNs by Marcelloni et al. [14] while an example of lossy compression in WSNs is the Lightweight Temporal Compression (LTC) scheme proposed by Schoellhammer et al. [15].

In general, most of the works on data compression applied to WSNs analyze the impact of the compression ratio in energy savings. However, Ying et al. [16], propose a new metric, called Energy-Saving Benefit (ESB) which is able to measure when compression wastes energy. The authors argue that compression ratio and time complexity are not enough to satisfactorily express the energy performance of the compression algorithms. Yu et al. [4] propose the concept of tunable compression that is able to tune the computation complexity of lossless data compression based on the energy availability. The concept comes from compression tools, such as gzip in which there are ten different levels of compression ratios. Since data compression and decompression in the nodes also dissipate energy, it is important to determine the energy savings achieved by different compression strategies. This fact is also expressed by Barr et al. [17]. They show that there is an increase in energy dissipation when compression is applied before transmission by using several typical compression tools. The main conclusion in these works is that data compression in WSN reduces the energy consumed in the transmission since less data is transferred to the sink, however, it should be kept in mind that energy is spent in

the compression/decompression process also. Chen et al. [18], investigate a similar tradeoff in joint routing and data aggregation and conclude via simulations that data compression reduces latency and energy consumption due to the transmission process. Tavli et al. [6], model dynamic data compression and decompression in conjunction with flow balancing in WSNs. They show that a dynamic model in which there a set of levels at which the node can choose to compress offers better performance in terms of network lifetime than compressing all data with the same algorithm or not compression the data at all.

Different from WSNs, Wireless Multimedia Sensor Networks (WMSNs), [19] (also called Visual Wireless Sensor Networks) have more stringent energy requirements because of the image quality, video coders, communication/computation expenses, and delays. In [20], the most important tradeoff has been reported as data quality versus energy consumption. It is also proved that using low cost video compression is beneficial in reducing transmission costs, as well as visual data transmission delay. Multimedia sensors are, then, good candidates to use smart compression schemes and WMSNs can benefit from the contextual privacy with data compression described in this work.

The literature on mathematical programming based modeling and analysis of WSNs is extensive and has grown rapidly in recent years. Providing a comprehensive overview of the published research on modeling WSNs through mathematical programming is beyond the scope of our work. We refer interested readers to the recent review papers on this topic [21, 22]. Indeed, most of the studies on network lifetime maximization in WSNs through mathematical programming achieve their maximization objective by optimizing the convergecast flow of data towards the base station. In fact, we also adopt a similar approach in this study. However, our study brings several novel and solid contributions to the literature on WSNs. First, we create an optimization framework to maximize network lifetime by jointly considering the privacy preservation (*i.e.*, the extent of the vulnerable area) and multi-level dynamic data compression, which has never been investigated in the literature. Second, we investigate the practical aspects of the problem (*e.g.*, what if only one compression level is allowed to be used or only a subset of nodes are capable of performing compression?). Third, We propose several novel data compression strategies and investigate the network lifetime performances of these strategies for WSNs providing stealth mode of operation. Fourth, we explore a large parameter space to uncover the tradeoffs involved in privacy preservation, multi-level data compression, and network lifetime through the numerical analysis of the proposed mathematical programming framework.

3. System Model

In this section we describe the system model, outline the assumptions, and present the Mathematical Programming framework.

3.1. Overview

The mitigation of compromising privacy concept obtained by transmission range control is illustrated in Figure 1. In this model, the WSN consists of nodes distributed over a Sensing Domain (SD), with a Base Station positioned at the center of SD. Each sensor node is able to sense in a radius r_s and we assume that its radio range, denoted as r_i, is larger than the sensing radius (*i.e.*, $r_i > r_s$). In a dense deployment case, the furthest nodes with respect the sink delimit the border of the sensing area (*i.e.*, if (x_i, y_i) is the location of a node and $(x-x_i)^2+(y-y_i)^2 \leq r_s^2$ is the sensing region of the node, the union of the sensing regions of all nodes will form the sensing domain). Since, the SD can be of any shape, for clarity and without loss of generality, we will consider a disk shaped SD of radius R_S with a sink, labeled as node-1, located at the center of the disk.

Since the radio range of a node fulfils that $r_i > r_s$, nodes near the border of the SD that transmit data can be monitored by an adversary that lies outside the SD area. As a matter of fact, this will be true for all the nodes whose location (x_i, y_i) meet the condition $\sqrt{(x_i^2 + y_i^2)} + r_i > R_S$. Let us define this area at which an adversary can observe data generated at the SD, the Vulnerable Domain (VD). Again for clarity, we consider that this area is limited by a radius R_v that defines the limit at which any packet generated at the SD area can not be leaked. Then, any adversary who is located outside the SD region and inside the R_v radius and who has similar capability radios as sensor nodes can sense packets generated at the Sensing Domain. The Vulnerable Domain (VD) will then be an annulus of area $A_{VD} = \pi(R_v^2 - R_s^2)$, and the difference R_u=R_v-R_s is defined as the Unobservability Margin. The larger the R_u is, the larger the VD becomes. Increasing VD increases the probability that the adversary is able to eavesdrop.

Remembering that r_i is the radio range of a node-i, increasing the transmission power will increase the Unobservability Margin R_u. But, on the other hand, the number of hops towards the sink is reduced, therefore, it can be possible to reach the sink in one hop. Obviously, transmission power control has a great impact on network lifetime and in the size of the VD area. We consider a contextual privacy topology model in order to study the relation between network lifetime and the extent of the Unobservability Margin. In this model, Figure 1, the maximum transmission range of a node-i is its distance to the VD area (*i.e.*, $R_{max,i} = |R_v - r_i|$). Then, in this model, nodes have different maximum transmission ranges.

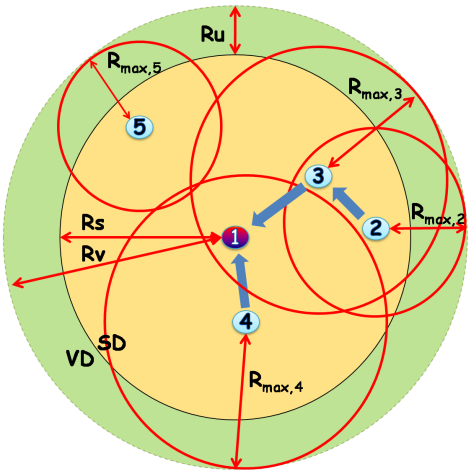


Figure 1: The contextual privacy topology model.

The main goal of this study, then, is to find the optimal flow assignment and data compression strategy that maximizes lifetime for a given VD area. In other words, what is the impact of decreasing the VD area in the lifetime of the network and how can we maximize the network lifetime by utilizing appropriate compression and flow balancing strategies?

3.2. Energy Model

The energy model used is the classical energy model defined by Heinzelman et al. [23], in which the amount of energy consumed to transmit a bit is defined as $P_{tx,ij} = \rho + \varepsilon d_{ij}^{\alpha}$, where ρ models the energy dissipation on electronic circuitry, ε denotes the transmitter's efficiency, α represents the path loss exponent and d_{ij} is the distance between node-i and node-j. Moreover, the amount of energy to receive a bit is represented as $P_{rx} = \rho$.

3.3. Data Flow Model

The network topology is defined as a directed graph $G = (V, A)$, where V is the set of nodes deployed in the SD (*i.e.*, N=$|V|$ is the number of nodes including the sink). The set W is defined as the set of nodes without counting the sink. We assume a convergecast traffic pattern (*i.e.*, all traffic flows from the sensors towards the sink). Let us define A as the set of arcs in the graph: $A = \{(i, j) : i \in W, j \in V - \{i\}\}$. A path $\mathcal{P}_i$ is a sequence of arcs from sensor i to the sink from which the traffic flows. Each node-i generates s_i units of raw data per unit time. The amount of traffic that it is sent from one node-i to another node-j is denoted by f_{ij}.

Data compression has been proposed as a technique to minimize the amount of data to be sent to the sink which has a potential to reduce communication energy dissipation. Yu et al, [4], propose to intelligently compress the raw data at different levels. The idea is that some compression tools (*e.g.*, gzip) support more than one level of compression. However, the higher the compression ratio is, the higher the energy dissipation is.

In this study, we use the data compression model introduced in [6], where the authors investigate strategies to optimize dynamic compression and flow balancing jointly to improve network lifetime. Their analysis show that by using dynamic compression it is possible to obtain significantly higher system lifetime than the achievable lifetime by pure strategies. In this dynamic data compression model, data compressed at a particular compression level can be transformed into another compression level by first decompressing the data and re-compressing them at another level. In the model, there are multiple options at each node for the optimization of system lifetime. It is emphasized that using different combinations of these below given options is possible for each node. The compression options available for the sensor nodes are itemized as follows:

- Raw data can be broken into branches and compressed at different compression levels.
- Compressed data at a specific level can be decompressed to raw data and re-compressed at different levels.
- Raw or compressed data can be forwarded directly or via other nodes to the base station.

Let us define a compression/decompression scheme in which there are K compression/decompression levels. Each level-k is characterized by a compression ratio γ_k (respectively a decompression ratio of $1/\gamma_k$). The energy consumption to compress 1 bit of data in the level-k is P_{cp}^k while the energy consumption to decompress 1 bit of data in the level-k is P_{dc}^k. In order to account for multiple compression/decompression levels, it is possible to define a virtual node for each compression level, called node-π_k, and a virtual node for each decompression level, called node-ω_k.

Now, the amount of raw data at node-i to be compressed at level-k is denoted as $f_{i\pi}^k$. The amount of compressed data at node-i for the level-k is denoted as $g_{\pi i}^k$. The amount of compressed data at node-i for the level-k sent for decompression to the virtual node-ω_k is denoted as $g_{i\omega}^k$. The amount of raw data generated by decompression at node-i by the virtual node-ω_k is denoted as $f_{\omega i}^k$. Finally, let us denote as

g_{ij}^k the amount of data that flows from node-i to node-j compressed at level-k. Figure 2 shows a network with 3 nodes and 2 levels for compression/decompression of data. In this example we can observe that node-2:

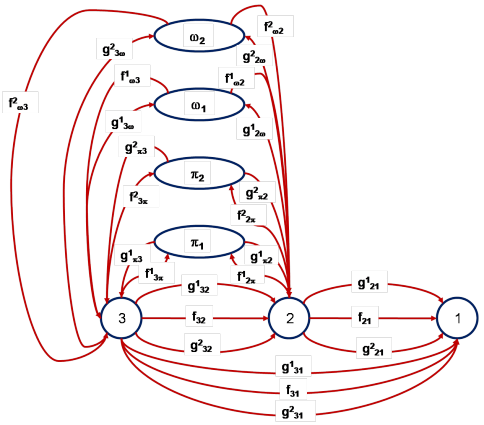


Figure 2: Data Compression/Decompression flow model.

(i) receives f_{32} units of raw data from node-3. It also receives g_{32}^1 and g_{32}^2 units of data compressed at level-1 and level-2, respectively, from node-3.

(ii) sends $f_{2\pi}^1$ and $f_{2\pi}^2$ units of raw data to be compressed at level-1 and level-2 at the virtual node-π_1 and node-π_2, respectively.

(iii) sends $g_{2\omega}^1$ and $g_{2\omega}^2$ units of compressed data to be decompressed at level-1 and level-2 at the virtual node-ω_1 and node-ω_2, respectively.

(iv) receives $g_{\pi 2}^1$ and $g_{\pi 2}^2$ units of compressed data at level-1 and level-2 from the virtual node-π_1 and node-π_2, respectively.

(v) receives $f_{\omega 2}^1$ and $f_{\omega 2}^2$ units of decompressed data at level-1 and level-2 from the virtual node-ω_1 and node-ω_2, respectively.

(vi) sends f_{21} units of raw data, g_{21}^1 and g_{21}^2 of compressed data at level-1 and level-2, respectively, to node-1.

3.4. Data Compression Strategies

Having laid the foundations of our framework, we will present the data compression strategies considered in this study. We employ five data compression strategies which are No Compression (NC) strategy, Always Compression (AC) strategy, Optimal Compression (OC), Optimal Single Level Compression (OSLC), and Limited Compression (LC). The first of these strategies are proposed and analyzed in [5, 6]. However, these models do not account for some of the inherent

limitations of WSNs. For example, it is possible that not all nodes have the capability to compress data. LC strategy is proposed to model such a practical limitation. Furthermore, utilizing different compression levels for each node brings extra overhead and in practical WSN deployments it is desirable to use a single data compression level for all sensor nodes which can be modeled by using the OSLC strategy. The compression strategies used in this study are itemized as follows:

- **No Compression (NC):** All data generated at the sensor nodes are conveyed to the base station without any compression.
- **Always Compression (AC):** All nodes compress their generated data by using a single compression level (*i.e.*, there is only one compression level utilized for the whole network).
- **Optimal Compression (OC):** Each node can divide the data it generates into parts and compress each part by using the optimal compression level. Some portion of the data can be chosen to be kept raw also.
- **Optimal Single Level Compression (OSLC):** In this strategy, the raw data can be divided in at most two parts. While one part of data has to be compressed at one level, the other part of the data may not be compressed. The other option, all data can be compressed at one level or all data is not compressed. In other words, if each node has one option for the selection of compression level, this strategy looks for optimal compression level to achieve maximum lifetime.
- **Limited Compression (LC):** In this strategy, only a limited number of nodes has the capability of data compression. Hence, effect of limiting number of nodes that has the capability of data compression on the lifetime WSN is revealed by using this strategy.

NC, AC, and OC strategies are modeled by using LP whereas OSLC and LC strategies are modeled by using MIP. Table 1 gives the compression levels and their energy dissipation values for tunable compression and decompression, [4, 6, 17]. These values are used in our LP and MIP Models described in Section 3.5. In this table, compression ratios, relative energy dissipation values and relative decompression energy dissipation values are taken from [4] and [17]. Moreover, relative energy values are scaled with the (JPEG) compression energy described in [20] for VWSNs (Visual Wireless Sensor Networks). Although, these values are taken as the baseline for our evaluations, other representative values of sensor hardware and software platforms can be used in our model, as well.

Table 1: Data Compression (Cmp) and Decompression (Decmp) Energy.

Cmp level k	Cmp energy P_{cp}^{k}	Cmp ratio γ_k	Decmp energy P_{dc}^{k}
1	360 nJ	0.430	90 nJ
2	380 nJ	0.385	95 nJ
3	440 nJ	0.365	110 nJ
4	540 nJ	0.355	135 nJ
5	600 nJ	0.350	150 nJ

3.5. Mathematical Programming Framework

In this subsection, we first present a novel LP model which forms the base for the rest of our formulations. Later, by including additional constraints we will synthesize LP and MIP models representing the strategies presented in Section 3.4. LP and MIP are widely used methods for finding the maximum or minimum value of a linear objective function under a set of linear constraints. Variables in an LP model take real values and some of the variables in an MIP model can be integers but all the relations between the variables in each model are linear. Table 2 describes all the parameters used in our framework. The optimization problem for maximizing lifetime (t) is presented in Figure 3. The lifetime of the WSN is described as the lifetime of the first node that consumes its battery energy completely [3, 6]. However, this definition should not be misinterpreted – when we examine the framework carefully it can be seen that to maximize the minimum lifetime, all nodes are forced to dissipate their energies in a balanced fashion, hence, sensor nodes in the network deplete their battery energies simultaneously.

All nodes except the base station are subject to all constraints defined in Figure 3 and explained in an itemized form as follows:

- Equations (1) and (2) state that all data flows are non-negative.
- Equation (3) states that raw data flow conservation condition is satisfied at each node.
- Equation (4) states that flow conservation condition for each node is satisfied at each compression level.
- Equation (5) relates compressed data with raw data via the compression ratio for each compression level.

Table 2: Terminology for LP/MIP Formulations

Symbol	Description	Symbol	Description
f_{ij}	Flow that shows the data sent from node-i to node-j	$E_{(cp,i)}$	Total energy spent to compress in node-i
$f_{i\pi}^{k}$	Raw data flow from node-i to be compressed at compression level-k	$E_{(dc,i)}$	Total energy spent to decompress data in node-i
f_{wi}^{k}	Raw data flow that has been decompressed at compression level-k in node-i	$E_{(rx,i)}$	Total energy spent to receive data in node-i
g_{ij}^{k}	level-k compressed flow from node-i to node-j	$E_{(tx,i)}$	Total energy spent to transmit data in node-i
$g_{\pi i}^{k}$	level-k compressed has been compressed in node-i	d_{ij}	Distance between node-i and node-j
$g_{i\omega}^{k}$	level-k compressed data is sent to be decompressed in node-i	R_{max}	The maximum distance that node-i can transmit its data and is related with power limitation of nodes
s_i	Amount of data (bits) generated per unit time in node-i	$R_{max,i}$	The maximum distance that node-i can transmit its data and is related with contextual privacy
e_i	Energy budget of the node-i	R_S	Sensing Domain radius
t	Network lifetime	R_V	Vulnerable Domain radius
P_{cp}^{k}	Energy spent to compress 1 bit of data in level-k	C_{Limit}	Limits maximum percentage of nodes that can be able to compress data
P_{dc}^{k}	Energy spent to decompress 1 bit of data in level-k	γ_k	level-k compression coefficient
$P_{(rx)}$	Energy spent to receive 1 bit of data	a_i^k	Binary variable to determine if compression level-k is used by node-i
$P_{(tx,ij)}$	Energy spent to transmit 1 bit of data from node-i to node-j	b_i	Binary variable to determine whether node-i compresses any data or not
ρ	Energy dissipated by the hardware	NVA	Normalized Vulnerable Area
ϵ	Efficiency factor	ApN	Area per node
α	Path loss exponent	M	Big number
λ	Packet error probability		

Maximize t
Subject to:

$$f_{ij} \geq 0, f_{i\pi}^k \geq 0, f_{\omega i}^k \geq 0 \quad \forall i \in W, \forall j \in V, \forall k \in K \tag{1}$$

$$g_{ij}^k \geq 0, g_{\pi i}^k \geq 0, g_{i\omega}^k \geq 0 \quad \forall i \in W, \forall j \in V, \forall k \in K \tag{2}$$

$$\sum_{j \in V} f_{ij} - \sum_{j \in W} f_{ji} + \sum_k f_{i\pi}^k - \sum_k f_{\omega i}^k = s_i t \ \ \forall i \in W \tag{3}$$

$$\sum_{j \in V} g_{ij}^k - \sum_{j \in W} g_{ji}^k + g_{i\omega}^k = g_{\pi i}^k \ \ \forall i \in W, \forall k \in K \tag{4}$$

$$g_{\pi i}^k = \gamma_k f_{i\pi}^k \ \ \forall i \in W, \forall k \in K \tag{5}$$

$$f_{\omega i}^k = \frac{1}{\gamma_k} g_{i\omega}^k \ \ \forall i \in W, \forall k \in K \tag{6}$$

$$E_{(cp,i)} = \sum_{k \in K} P_{cp}^k f_{i\pi}^k \ \ \forall i \in W \tag{7}$$

$$E_{(dc,i)} = \sum_{k \in K} P_{dc}^k g_{i\omega}^k \ \ \forall i \in W \tag{8}$$

$$E_{(rx,i)} = P_{rx} \sum_{j \in W} (f_{ji} + \sum_{k \in K} g_{ji}^k) \ \ \forall i \in W \tag{9}$$

$$E_{(tx,i)} = \sum_{j \in V} P_{tx,ij} (f_{ij} + \sum_{k \in K} g_{ij}^k) \ \ \forall i \in W \tag{10}$$

$$E_{(cp,i)} + E_{(dc,i)} + E_{(rx,i)} + E_{(tx,i)} \leq e_i \ \ \forall i \in W \tag{11}$$

$$f_{ij} = 0, \text{ if } d_{ij} > R_{(max,i)} \quad \forall i \in W, \forall j \in V, \forall k \in K \tag{12}$$

$$g_{ij}^k = 0, \text{ if } d_{ij} > R_{(max,i)} \quad \forall i \in W, \forall j \in V, \forall k \in K \tag{13}$$

Figure 3: The base LP model.

- Equation (6) relates decompressed data with raw data via the compression ratio for each decompression level.
- Equation (7) gives the energy dissipation on compressing data at each node.
- Equation (8) gives the energy dissipation on decompressing data at each node.
- Equation (9) gives the energy dissipation on data reception (both raw and

compressed data) at each node.

- Equation (10) gives the energy dissipation on data transmission (both raw and compressed data) at each node.
- Equation (11) states that the energy dissipation of each node is upper bounded by the initial energy.
- Equations (12) and (13) state that node-$i \in V$ can not communicate with node-$j \in W$, if node-j is located beyond the maximum transmission range of node-i. Note that the maximum transmission range ($R_{max,i}$) is determined by the contextual privacy constraint.

The base LP model in Figure 3 is used for Optimal Compression (OC) strategy in which every node can be able to choose one or more than one compression level or they can choose not to compress data. $R_{max,i}$ is used to provide contextual privacy to the nodes and prevents nodes sending data out of the Vulnerable Domain. In addition to $R_{max,i}$ limitation, nodes may have a transmission power threshold, R_{max}, imposed by the transceiver characteristics (*e.g.*, power amplifier limits). We assume that deployed sensor nodes are the same type of nodes and they have the same transmission power threshold (*i.e.*, the same maximum transmission range). We develop an optimization model for this case by adding two constraints (Equation 14 and 15) to the base LP model in Figure 3.

$$f_{ij} = 0, \text{ if } d_{ij} > R_{(max)} \qquad \forall i \in W, \forall j \in V, \tag{14}$$

$$g_{ij}^{k} = 0, \text{ if } d_{ij} > R_{(max)} \qquad \forall i \in W, \forall j \in V, \forall k \in K. \tag{15}$$

Equations (14) and (15) are similar to the equations (12) and (13). Moreover, if R_{max} and $R_{max,i}$ are used together in the same model, then it is obvious that $R_{max,i} \leq R_{max}$ since R_{max} determines the maximum transmission power that the node may achieve.

The LP model described in Figure 3 should be extended to accommodate different data compression strategies defined in subsection 3.4 by introducing additional constraints. The NC strategy dictates preventing flows of compressed data between nodes. Thus, the NC optimization problem for maximizing lifetime of the WSN is constructed by augmenting equation (16) to the base LP model.

$$g_{ij}^{k} = 0, \qquad \forall i \in W, \forall j \in V, \forall k \in K. \tag{16}$$

Always Compression (AC) strategy is the complete opposite of the NC strategy. The AC strategy always compress raw data by choosing one of the available compression levels. To model the AC strategy, first, prevention of flows of raw

data between nodes should be incorporated to the base LP model and then a specific compression level should be assigned. Therefore, two additional constraints are required. Our objective again is maximization of lifetime by providing contextual privacy with data compression for AC strategies, subject to the constraints presented in Figure 3 in conjunction to Equations (17) and (18). Note that k_{AC} denoted the selected compression level for the whole network. For example, if all nodes compress all their generated data at compression level-3 (such a case is denoted as AC3) then $k_{AC} = 3$.

$$f_{ij} = 0, \qquad \forall i \in W, \forall j \in V, \tag{17}$$

$$g_{ij}^{k} = 0, \text{ if } k \neq k_{AC} \qquad \forall i \in W, \forall j \in V, \forall k \in K. \tag{18}$$

In the Optimal Compression (OC) strategy, each node can use different compression levels in addition to the option of no compression. For example, one possible arrangement for node-i is that raw data can be divided in six parts. One part can be sent to the other nodes without applying compression and the other five parts can be sent to the other nodes after compressing each part with different compression level. Yet another arrangement for node-i is that all the data can be sent to other nodes without applying compression. It is possible to come up plenty of arrangements for each node when OC strategy is chosen. On the other hand, there is only one option for the AC strategy, every node has to compress data with the predetermined compression level.

Optimal Single Level Compression (OSLC) strategy is in between OC and AC strategies. Each node can divide its data into at most two parts. One part can be the raw data and the other part should be compressed by using only one of the available compression levels. Of course, the whole data can be compressed by using a single compression level (no raw data is left) or all data can be kept as raw data (no compression at all). The arrangement of partitioning data, selecting the optimal compression level or not compressing is decided by the optimization framework in such a way that network lifetime is maximized. To model OSLC strategy, two additional constraints should be created – Equations (19) and (20).

$$f_{i\pi}^{k} \leq M a_{i}^{k}, \qquad \forall i \in W, \forall k \in K, \tag{19}$$

$$\sum_{k \in K} a_{i}^{k} \leq 1, \qquad \forall i \in W. \tag{20}$$

Equation (19) is defined to link continuous variables $f_{i\pi}^{k}$'s with the binary variables a_{i}^{k}'s. M is a large constant used to ensure that the right side of Equation (19) is always larger than $f_{i\pi}^{k}$ when $a_{i}^{k} = 1$, therefore, an alternative definition of M is

that $M = max(f_{i\pi}^k)$. Note that a_i^k is zero if there is no data flow on $f_{i\pi}^k$ and a_i^k is unity if there is non-zero flow on $f_{i\pi}^k$. In other words, Equation (19) ensures that a compression level-k is marked as chosen for compressing data at node-i only if the amount of raw data sent to the virtual node-π_k at node-i is non zero ($a_i^k = 1$ if $f_{i\pi}^k > 0$). Equation (20) limits the number of compression levels that are used by each node to one. In other words, if a portion of raw data has to be compressed, node-i has to use one compression level. Equations presented in Figure 3 combined with Equations (19) and (20) form the optimization model for OSLC. Since Equations (19) and (20) include binary variables, this is a Mixed Integer Programming (MIP) model.

The Limited Compression (LC) strategy is used to investigate how the lifetime of nodes is affected if only a subset of the deployed nodes is able to compress data. The LC strategy optimally selects the set of nodes that can compress data. The LC strategy is obtained by adding Equations (21) and (22) to the equations in Figure 3.

$$\sum_{k \in K} f_{i\pi}^k \leq M b_i, \qquad \forall i \in W, \tag{21}$$

$$\sum_{i} b_i \leq C_{Limit}, \qquad \forall i \in W. \tag{22}$$

Equation (21) specifies whether node-i compresses raw data or not. If node-i compresses raw data, the value of binary variable b_i is set to unity. If $b_i = 0$ then node-i is not one of the nodes selected to compress data. C_{Limit} in Equation (22) is the maximum percentage of number of nodes that are able to compress raw data. Again the objective of the model is maximizing lifetime. Since Equations (21) and (22) include binary variables, this model also is an MIP model.

4. Analysis

In this section we present the results of numerical analysis of the proposed data compression strategies to characterize the effects of these strategies on network lifetime for WSNs operating in stealth mode. The compression strategies are OC, OSLC, LC, and five different compression levels of AC (AC1, AC2, AC3, AC4, and AC5) strategies. Furthermore, to emphasize the impacts of compression methods, we also include the uncompressed data (*i.e.*, NC) results into our analysis. Contextual privacy objective is achieved by controlling the maximum data transmission range for each node ($R_{max,i}$). We use GAMS (General Algebraic Modeling System) for the numerical analysis of LP and MIP models. GAMS consists of high performance solvers for solving LP and MIP models efficiently. In our analysis, each problem is averaged over 125 random topologies.

The number of deployed nodes is varied from 75 to 125. Each node-i generates s_i units of raw data per unit time (1 bps). Each node has 2 KJ initial energy. All nodes can communicate with the base station through either a direct or a multi-hop path. We use the standard values of receiver constant (ρ is 50 nJ/bit), transmitter constant (ε is 100 pJ/bit/m^2), and the path loss exponent ($\alpha = 2$), as in [12, 24]. The parameters used in the analysis are presented in Table 3.

Table 3: Parameter values

Parameter	**Values**
ρ	50 nJ/bit
ε	100 pJ/bit/m^2
α	2
N	75–125
NVA	0 - 3
ApN	100 m^2–900 m^2
e_i	2 KJ
s_i	1 bit/s
C_{limit}	$0.1N$–$1N$
R_{max}	$0.3R_S$–R_S

We analyze the network lifetime as a function of Normalized Vulnerable Area (NVA), while maximizing the lifetime and applying different compression methods by varying node density. NVA is obtained by dividing the area of vulnerable domain to the area of sensing domain. The maximum NVA value is 3, because at NVA=3 all sensor nodes can reach the base station directly, hence, position dependent maximum transmission range constraint is effectively lifted for $NVA \geq 3$. In other words, any value of NVAlarger than 3 will be meaningless since transmitting over a distance larger than R_S is unnecessary for a disk shaped network, where the base station is located at the center. All lifetime values with the transmission range limitations are normalized with the lifetime values obtained when there is no transmission range limitation (*i.e.*, all lifetime values obtained in each case are normalized with maximum lifetime obtained in that case). All cases are analyzed for different ApN (Area per Node) topologies ($ApN = 100\ m^2$, 300 m^2, and 900 m^2). ApN is obtained by dividing the total network area (*i.e.*, the area of the SD) by the number of nodes (N) in the network. Alternatively, the area of the SD is obtained by multiplying ApN by the number of nodes in the network.

The results are evaluated in two phases. At the first phase, we optimized data flows and analyzed lifetime versus NVA for different topologies, only considering the level of contextual privacy provided without using any compression strategy. At

the second phase, we optimized data flows while providing contextual privacy as in the first phase and analyzed the effects of applying data compression strategies (*i.e.*, OC, OSLC, LC and ACs) on lifetime for different scenarios.

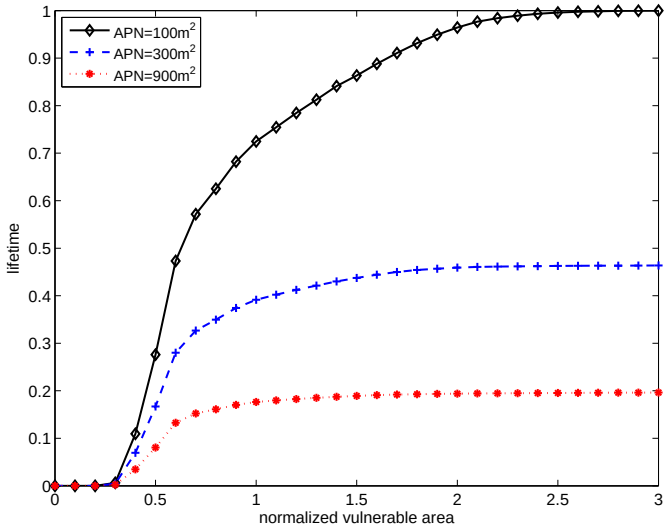


Figure 4: Normalized lifetime as a function of NVA for different ApN values ($N = 100$)

Figure 4 presents the first phase, where there is no data compression. Normalized lifetime is plotted as a function of NVA for different ApN values. Network lifetime decreases as ApN increases. For example, when $NVA = 1$, normalized lifetimes for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$ are 0.72, 0.39, and 0.17, respectively. Increasing ApN leads to larger distances among nodes, thus the energy cost of sending data to the base station increases which results in decrease in the lifetime. When nodes reach their maximum data transmission distance, we observe constant lifetimes for all three cases. Normalization is achieved by dividing all the lifetime values by the maximum lifetime.

In the second phase, effects of data compression strategies on lifetime for different ApN values are analyzed. The compression strategy acronyms used in the Figures are given in Table 4.

Figure 5(a) shows the lifetime change for different compression strategies for $ApN = 100\ m^2$. Figure 5(a) reveals that mandatory compression of all the collected data has a negative effect on the lifetime. OC provides the best network lifetimes for all NVA values and the maximum normalize lifetime is 1. All nodes mostly use one compression level when data is required to be compressed, hence, lifetime values obtained by OC and OSLC methods are almost the same for all NVA values. Also, it is clear that AC methods do not bring any significant gains

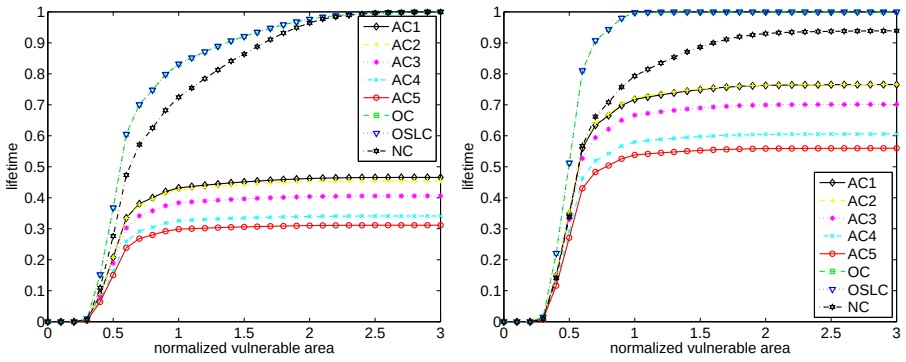
Table 4: Acronyms used in the Plots.

Acronyms	Compression Techniques
NC	No Compression
OC	Optimal Compression
OSLC	Optimal Single Level Compression
LC	Limited Compression
AC	Always Compression
AC1	Always Compression – Level-1
AC2	Always Compression – Level-2
AC3	Always Compression – Level-3
AC4	Always Compression – Level-4
AC5	Always Compression – Level-5

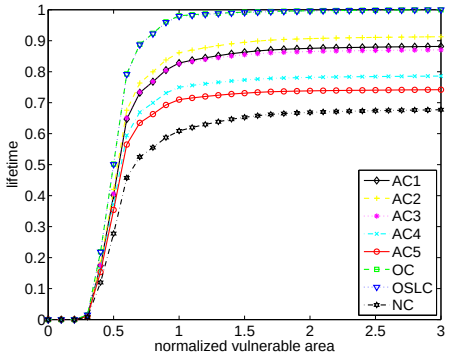
for this case (*i.e.*, NC results in higher lifetimes than the ones achieved by using AC). For example, when $NVA = 1$, normalized lifetimes for NC, OC, OSLC, AC1, AC2, AC3, AC4, AC5 strategies are 0.72, 0.83, 0.83, 0.43, 0.42, 0.38, 0.32, and 0.29, respectively.

Figure 5(b) presents the lifetime for different compression strategies when $ApN = 300\ m^2$. When we compare Figure 5(a) ($ApN = 100\ m^2$) with Figure 5(b) ($ApN = 300\ m^2$), especially, when the NVA values are smaller than unity, it is evident that compression helps getting higher lifetimes with increasing ApN values. On the other hand, NC is still the best strategy after OC and OSLC, Furthermore, lifetime values obtained by OC and OSLC strategies are almost the same for all NVA values for $ApN = 300\ m^2$. For example, when $NVA = 1$, normalized lifetimes for NC, OC, OSLC, AC1, AC2, AC3, AC4, AC5 are 0.79, 0.99, 0.99, 0.71, 0.72, 0.66, 0.58, and 0.53, respectively. For this case, the maximum normalize lifetime almost is half of the maximum normalized lifetime with $ApN = 100\ m^2$.

Figure 5(c) presents lifetimes for different compression methods for $ApN = 900\ m^2$. The figure shows that OC and OSLC strategies are the best strategies for this case, as well. On the other hand, AC strategies have comparatively higher lifetime values than their values at lower ApN's, which are close to OC values. For example, when $NVA = 1$, normalized lifetimes for NC, OC, OSLC, AC1, AC2, AC3, AC4, AC5 are 0.61, 0.98, 0.97, 0.86, 0.83, 0.83, 0.75, and 0.71, respectively. The difference between Figure 5(a) and Figure 5(c) highlights that when ApN value is high, using all compression strategies in the network results in increased lifetimes for all NVA values. Moreover, together with the high ApN, the increased distances among the nodes necessitates the utilization of compres-



(a) $ApN = 100\ m^2$ (b) $ApN = 300\ m^2$

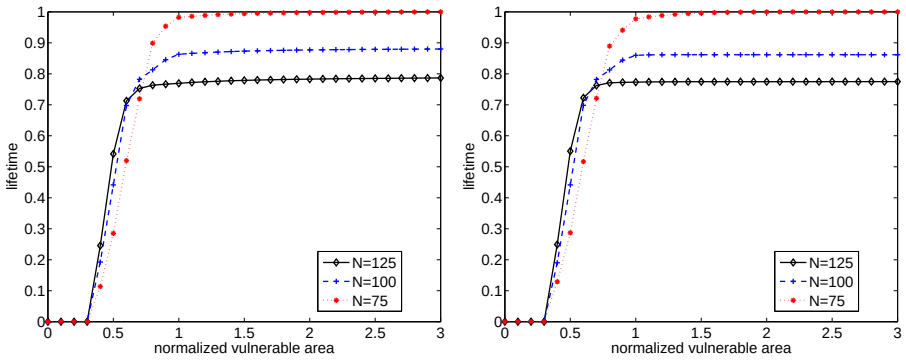


(c) $ApN = 900\ m^2$

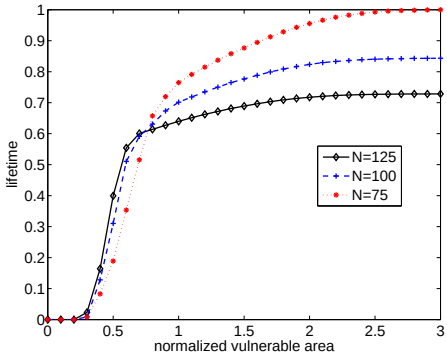
Figure 5: Effects of different compression strategies on normalized lifetime as a function of NVA for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$ ($N = 100$).

sion strategies to obtain higher lifetime values, hence, the disadvantage of AC over NC in Figure 5(a) and Figure 5(b) diminishes in Figure 5(c). For the case of $ApN = 900\ m^2$, the maximum lifetime used for the normalization is almost one third of the maximum normalized lifetime with $ApN = 100\ m^2$.

Figures 6(a), 6(b), and 6(c) show the effects of number of nodes on normalized lifetimes using OC strategy as a function of NVA for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$, respectively. While $NVA < 0.8$, there is a strong correlation between the number of nodes and the normalized lifetimes. In other words, as the number of nodes increases, the normalized lifetimes also increase. But after $NVA \geq 0.8$, there is an inverse relation between number of nodes and normalized lifetimes. This is because for smaller NVA ($NVA < 0.8$), disconnection probability of the network is higher for lower number of nodes that affects normalized lifetimes. After $NVA \geq 0.8$, there is almost no disconnection in the network and as the number of nodes increases the normalized lifetime decreases.



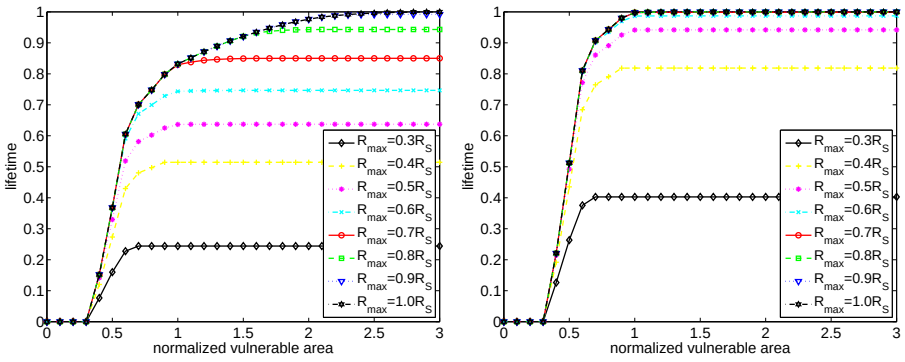
(a) $ApN = 100\ m^2$ (b) $ApN = 300\ m^2$



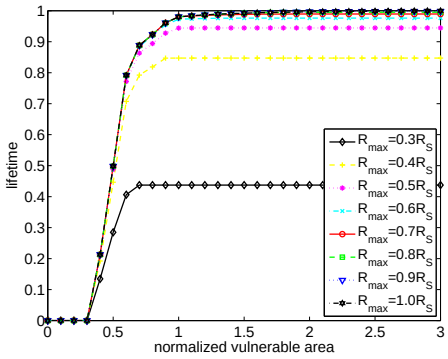
(c) $ApN = 900\ m^2$

Figure 6: Effects of number of nodes on normalized lifetime using OC strategy as a function of NVA for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$.

Figures 7(a), 7(b), and 7(c) show the effects of R_{max} on normalized lifetime using OC strategy as a function of NVA for $ApN = 100\,m^2$, $300\,m^2$, and $900\,m^2$, respectively. The number of nodes in the network is kept constant as 100 and R_{max} is chosen as proportional to the radius of the deployment area (R_S). The optimal operation of networks that are deployed in small areas is sending most of their data directly to the base station. Since direct communication with base station requires higher energy, as the area increases nodes tend to use multi-hop communication to send their data towards the base station. In Figure 7(a), when R_{max} constraint is not active (*i.e.*, R_{max}=R_S), most of the nodes in the network send most of their data directly to the base station. When R_{max} constraint ($R_{max} \geq 0.3R_S$) is active, R_{max} threshold prevents some of the nodes from sending data directly to the base station which leads to extra energy dissipation and lower lifetime. For example, when $NVA = 2$, the normalized lifetimes are 0.24, 0.51, 0.64, 0.75, 0.85, 0.94, 0.98, 0.98 for R_{max}=$0.3R_S$, R_{max}=$0.4R_S$, R_{max}=$0.4R_S$, R_{max}=$0.6R_S$, R_{max}=$0.7R_S$,



(a) $ApN = 100\ m^2$ (b) $ApN = 300\ m^2$



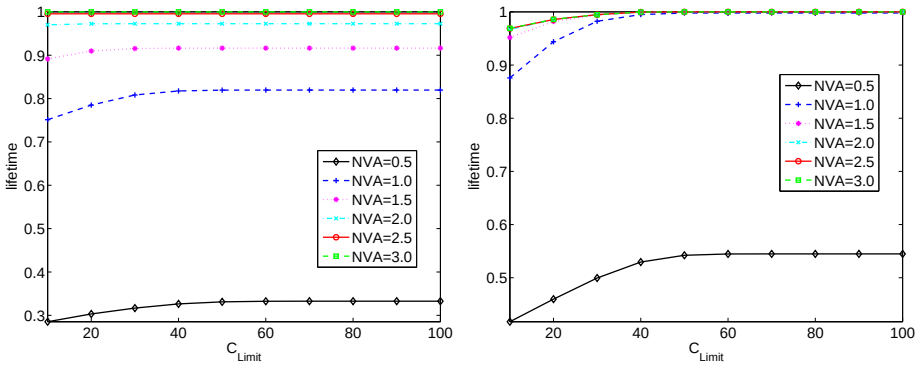
(c) $ApN = 900\ m^2$

Figure 7: Effects of R_{max} on normalized lifetime using OC strategy as a function of NVA for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$.

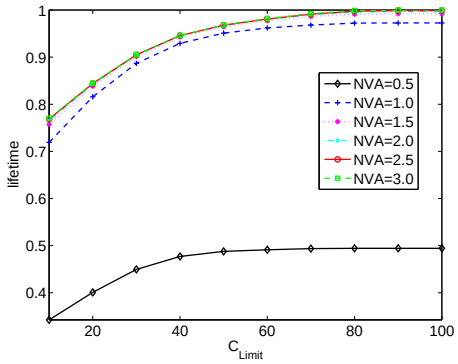
R_{max}=0.8R_S, R_{max}=0.9R_S, and R_{max}=R_S, respectively.

As the network size increases, the impact of R_{max} constraint on the lifetime becomes less visible. In figure 7(b) and 7(c), for R_{max} $\geq$0.6R_S, the change in network lifetime is negligibly low. The reason for such behavior is that for $R_{max} \geq$ 0.6R_S, $R_{max,i}$ constraint dominates R_{max} constraint. While R_{max} <0.6R_S, although $R_{max,i}$ constraint allows nodes sending data to relay nodes, R_{max} constraint prevents some of these nodes using some relay nodes. Hence, R_{max} manifests its impact by decreasing lifetime for R_{max} <0.6R_S.

Figures 8(a), 8(b), and 8(c) show the effects of limited compression (LC) strategy on normalized lifetime as a function of compression-limit (C_{limit}) for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$, respectively. The number of nodes in the network is kept constant as 100. In this part, we investigate the impact of limiting the number of nodes which are able to compress and decompress data on normalized lifetime. As stated before, because of high energy cost, the percentage



(a) $ApN = 100\ m^2$ (b) $ApN = 300\ m^2$



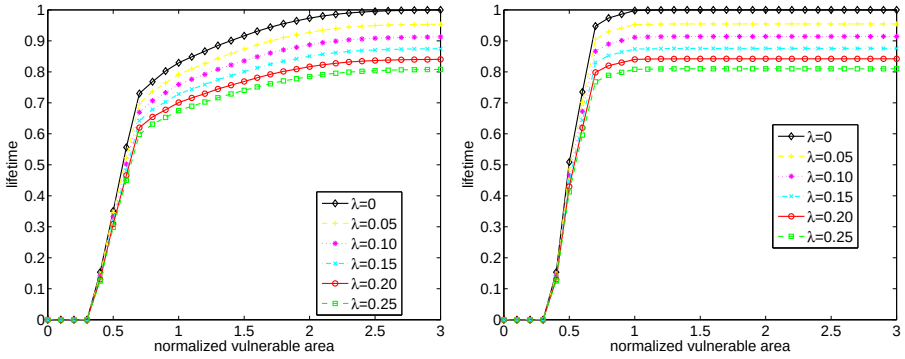
(c) $ApN = 900\ m^2$

Figure 8: Effects of limited compression strategy on normalized lifetime as a function of C_{limit} for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$.

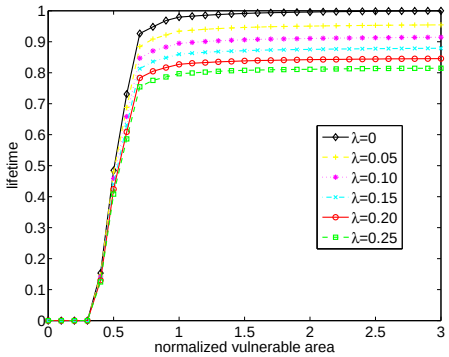
of data sent directly to the base station decreases as the area increases (*e.g.*, most of the sensor nodes in the $ApN = 100\ m^2$ network send most of their data directly to the base station). As shown in Figure 8(a), enforcing compression limit on the network does not result in a significant deviation from the optimal energy balancing flows because most of the nodes are able to send data directly to the base station with less energy. In other words, most of the nodes in the $ApN = 100\ m^2$ network does not need to use compression to achieve maximum lifetime. For example, even if only 10 % of the nodes (C_{limit}=10) are able to compress and decompress data, deviation from maximum lifetime obtained in the unrestricted case ($C_{limit} \rightarrow \infty$) are 14.21 %, 8.34 %, 2.71 %, 0.26 %, 0 %, 0 % for $NVA = 0.5$, $NVA = 1$, $NVA = 1.5$, $NVA = 2.0$, $NVA = 2.5$, $NVA = 3.0$, respectively.

For larger networks, ($ApN = 300\ m^2$ and $900\ m^2$), percentage of direct transmission to the base station is low and the nodes (especially ones farther away from the base station) tend to send most of their data to a limited number of relay nodes

to be conveyed to the base station. Also, the nodes tend to use compression in larger networks to reduce energy cost of sending data towards the base station. Therefore, enforcing compression limit in larger networks results in larger deviations from the maximum lifetime obtained in the unrestricted case ($C_{limit} \rightarrow \infty$). For $ApN = 100\ m^2$ network (figure 8(a)), when $NVA \geq 1.0$, enforcing compression limit does not prevent the network from achieving near optimal lifetime values, however, for $ApN = 300\ m^2$ network (figure 8(b)), when $NVA \geq 1.0$, maximum lifetime can only be achieved for C_{limit} $\geq$40. For $ApN = 900\ m^2$ network (figure 8(c)), when $NVA \geq 1.0$, maximum lifetime can only be achieved after C_{limit} $\geq$70.



(a) $ApN = 100\ m^2$ (b) $ApN = 300\ m^2$



(c) $ApN = 900\ m^2$

Figure 9: Effects of packet error probability on normalized lifetime as a function of NVA for $ApN = 100\ m^2$, $300\ m^2$, and $900\ m^2$.

Exploring the effects of packet losses on WSN lifetime is an important task for the validation of our system model. To incorporate the effects of packet losses we define a new variable λ which is the maximum probability of packet error at a link (i.e., if $\lambda = 0.10$ then the links in the network have packet error probabilities in the

range of $[0, 0.10]$). Furthermore, we set $s_i = 1024$ bits (128 Byte packets are generated at each node periodically) for this analysis. We obtained the optimal flows by setting $\lambda = 0$ and on the same topology we assign packet error probabilities randomly to each link. We further assume that once a packet is lost, it is retransmitted, therefore, the energy cost of transmitting and receiving a data packet is scaled with $\frac{1}{(1-\varphi)}$ where φ is the packet error probability on the link. For example, if $\varphi = 0.2$ for a particular link then the average energy cost of transmission and reception on the link is 25 % more than the energy costs when there is no packet losses. Figures 9(a), 9(b), and 9(c) show the effects of packet error probability on normalized lifetime as a function of NVA for $ApN = 100\ m^2$, 300 m^2, and 900 m^2, respectively. The number of nodes in the network is kept constant as 100 and λ is chosen between 0 % (no error) and 25 %. As λ increases the normalized network lifetime decreases monotonically. For example, when $NVA = 3$ and ApN=100, the normalized lifetimes are 0.96, 0.91, 0.87, 0.84, 0.81 for $\lambda = 0.05$, $\lambda = 0.10$, $\lambda = 0.15$, $\lambda = 0.20$, and $\lambda = 0.25$, respectively. Hence, the main conclusion of this analysis for validating our model is that packet errors has a significant impact on the network lifetime because there is an effective increase on the cost of communicating data due to retransmissions. However, except for the relative decrease with increasing λ, the effects of privacy preservation constraint (*i.e.*, NVA) on network lifetime do not change significantly from packet errors (*i.e.*, network lifetime characteristics as functions of NVA do not exhibit significant variations for different λ values).

5. Conclusions

In this paper, we investigate the effects of providing contextual privacy on network lifetime in WSNs operating in stealth mode by limiting the transmission power levels of sensor nodes in a position dependent fashion. To mitigate the adverse effects of contextual privacy measures on maximum achievable lifetime we propose the employment of various data compression strategies. To analyze the benefits of these strategies qualitatively in prolonging the network lifetime of WSNs operating in stealth mode, we created a mathematical programming framework. We explored the parameter space by employing the developed mathematical programming framework encompassing both LP and MIP models. A brief summary of our findings are itemized as follows:

- The major conclusion of this study is that optimal utilization of data compression can reduce the energy cost of providing contextual privacy in WSNs, significantly.

- Under certain conditions, it is possible to obtain near optimal lifetime values by utilizing only a small percentage of optimally selected sensor nodes performing data compression.
- Employing a single optimal compression level strategy results in network lifetime values in close vicinity of the network lifetimes obtained by using a strategy that utilizes all available compression levels.

6. Acknowledgements

This research is supported, in part, by projects TIN2013-47272-C2-2 and SGR2014-881.

References

[1] N. Li, N. Zhang, S. K. Das, B. Thuraisingham, Privacy preservation in wireless sensor networks: A state-of-the-art survey, Ad Hoc Networks 7 (2009) 1501–1514.

[2] M. Conti, J. Willemsen, B. Crispo, Providing source location privacy in wireless sensor networks: A survey, IEEE Communications Surveys Tutorials 15 (2013) 1238–1280.

[3] B. Tavli, M. M. Ozciloglu, K. Bicakci, Mitigation of compromising privacy by transmission range control in wireless sensor networks, IEEE Communications Letters, 14 (2010) 1104–1106.

[4] Y. Yu, B. Krishnamachari, V. Prasanna, Data gathering with tunable compression in sensor networks, IEEE Transactions on Parallel and Distributed Systems 19 (2008) 276–287.

[5] R. Zilan, T. H. Ozdemir, B. Tavli, J. M. Barcelo-Ordinas, Prolonging wireless sensor network lifetime in stealth mode through intelligent data compression, in: Proc ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks (PE-WASUN), 2013, pp. 105–112.

[6] B. Tavli, I. Bagci, O. Ceylan, Optimal data compression and forwarding in wireless sensor networks, IEEE Communications Letters, 14 (2010) 408–410.

[7] Y. Fan, Y. Jiang, H. Zhu, X. Shen, An efficient privacy-preserving scheme against traffic analysis attacks in network coding, in: Proc. IEEE Conference on Computer Communications (INFOCOM), 2009, pp. 2213–2221.

[8] C. Ozturk, Y. Zhang, Source-location privacy in energy-constrained sensor network routing, in: Proc. ACM workshop on Security of ad hoc and sensor networks (SASN), 2004, pp. 88–93.

[9] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, Entrapping adversaries for source protection in sensor networks, in: Proc. International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2006, pp. 10–34.

[10] X. Hong, P. Wang, J. Kong, Q. Zheng, jun Liu, Effective probabilistic approach protecting sensor traffic, in: Proc. IEEE Military Communications Conference (MILCOM), volume 1, 2005, pp. 169–175.

[11] N. Dutta, A. Saxena, S. Chellappan, Defending wireless sensor networks against adversarial localization, in: Proc. International Conference on Mobile Data Management (MDM), IEEE, 2010, pp. 336–341.

[12] Z. Cheng, M. Perillo, W. Heinzelman, General network lifetime and cost models for evaluating sensor network deployment strategies, IEEE Transactions on Mobile Computing 7 (2008) 484–497.

[13] T. Srisooksai, K. Keamarungsi, P. Lamsrichan, K. Araki, Practical data compression in wireless sensor networks: A survey, Journal of network and computer applications 35 (2012) 37–59.

[14] F. Marcelloni, M. Vecchio, Enabling energy-efficient and lossy-aware data compression in wireless sensor networks by multi-objective evolutionary optimization, Information Sciences 180 (2010) 1924–1941.

[15] T. Schoellhammer, B. Greenstein, E. Osterweil, M. Wimbrow, D. Estrin, Lightweight temporal compression of microclimate datasets, Proc. IEEE International Conference on Local Computer Networks (LCN) (2004) 224–516.

[16] B. Ying, Y. Liu, H. Yang, H. Wang, Evaluation of tunable data compression in energy-aware wireless sensor networks, Sensors 10 (2010) 3195–3217.

[17] K. C. Barr, K. Asanović, Energy-aware lossless data compression, ACM Trans. Comput. Syst. 24 (2006) 250–291.

[18] M. Chen, M. L. Fowler, The importance of data compression for energy efficiency in sensor networks, in: Proc. Conference on Information Sciences and Systems, Hopkins University, 2003.

[19] B. Tavli, K. Bicakci, R. Zilan, J. M. Barcelo-Ordinas, A survey of visual sensor network platforms, Multimedia Tools Appl. 60 (2012) 689–726.

[20] C. F. Chiasserini, E. Magli, Energy consumption and image quality in wireless video-surveillance networks, in: Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), volume 5, 2002, pp. 2357–2361.

[21] F. Ishmanov, A. S. Malik, S. M. Kim, Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): a comprehensive overview, European Transactions on Telecommunications 22 (2011) 151–167.

[22] A. Gogu, D. Nace, A. Dilo, N. Meratnia, Review of optimization problems in wireless sensor networks, in: J. Hamilton Ortiz (Ed.), Telecommunications Networks - Current Status and Future Trends, InTech, 2012, pp. 153–180.

[23] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, An application specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (2002) 660–670.

[24] S. Ergen, P. Varaiya, On multi-hop routing for energy efficiency, IEEE Communications Letters 9 (2005) 880–881.