

MASARYK UNIVERSITY
FACULTY OF INFORMATICS



Evaluation of privacy preserving protocols

BACHELOR THESIS

Robert Zahradníček

Brno, Autumn 2012

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Advisor: RNDr. Jiří Kůr

Acknowledgement

I would like to thank RNDr. Jiří Kůr for his advices and help during writing this thesis.

Abstract

Aim of this thesis is to study and describe privacy protection issues in the wireless sensor networks, its primary focus is on the privacy preservation against global eavesdropper and the evaluation of these techniques. Practical part of this thesis is comprised of implementation of privacy preserving techniques and their evaluation by means of selected performance metrics.

Keywords

Wireless sensor network, privacy, privacy-preserving protocols, source-simulation, periodic-collection, metrics

Contents

1	Introduction	2
2	Wireless sensor network	3
2.1	<i>Structure and design</i>	3
2.1.1	Hardware platform	3
2.1.2	Software platform	4
2.1.3	Communication protocols platform	5
2.2	<i>Applications</i>	5
3	Privacy-preservation in wireless sensor networks	7
3.1	<i>Panda-Hunter game</i>	7
3.2	<i>Adversary models</i>	8
3.2.1	Internal adversary	8
3.2.2	External adversary	8
3.2.3	Local eavesdropper	8
3.2.4	Global eavesdropper	9
3.2.5	Passive adversary	9
3.2.6	Active adversary	9
3.3	<i>Taxonomy of privacy in WSN</i>	9
3.3.1	Data-oriented privacy	9
3.3.2	Context-oriented privacy	10
3.4	<i>Privacy attacks</i>	10
3.4.1	Traffic analysis	10
4	Privacy preserving protocols	11
4.1	<i>Periodic collection protocol</i>	11
4.1.1	Protocol description	11
4.2	<i>Source simulation protocol</i>	12
4.2.1	Protocol description	12
5	Evaluation	14
5.1	<i>Metrics</i>	14
5.1.1	Performance metrics	14
5.2	<i>Testing platform</i>	16
6	Results	17
6.1	<i>Energy consumption</i>	17
6.2	<i>Communication cost</i>	19
6.3	<i>Message latency</i>	21
6.4	<i>Memory usage</i>	22
6.5	<i>Reliability</i>	23
6.6	<i>Availability</i>	24
7	Conclusion	25
A	Content of attached CD	29

Chapter 1

Introduction

Security in wireless sensor networks is active and wide-open field of study. While initially main focus was on effective functionality of these networks [16] recently the focus has changed to security issues [29] wireless sensor networks posses.

Because of rapid development in a field of wireless sensor networks, number of their possible applications increase as well. With wide area of possible applications for technologies of wireless sensor networks are bound also many hostile intentions. These use cases also envelop sending potentially private information through the motes in the network. Therefore a lot of work has been focused on development of key distribution infrastructures for usage of encryption to ensure confidentiality, integrity and authenticity of messages transmitted between motes in the wireless sensor networks. Although protection of data payloads and therefore the actual content of messages is very important in sensor networks, there still remains contextual information of motes communication. This contextual communication patterns can be very sensitive and their protection crucial for successful operation of the sensor network. By observing communication patterns malicious adversary can pinpoint locations of events or sensor nodes. These events can be as simple as change in some physical phenomena like temperature, pressure, humidity etc. or they can be generated for example by change in vital functions of monitored patient in the hospital. In the first example there does not have to be anything sensitive about information transmitted through the wireless sensor network and so enforcing preservation of privacy of contextual information is not immediately necessary. The second example however shows rather useful application of wireless sensor networks which brings with itself a need to protect privacy of monitored objects too, as well as protection of content of messages communicated over the network.

Extensive work has been done to develop effective privacy preserving communication protocols. Hence not only monitored object privacy may be at concern but also location privacy of key motes of the network is desired. Various facts have to be concerned in design of such protocol, mainly amount of overheads this protocol will bring to the network operation cycles or which model of adversary it will be focused on, etc. For purposes of evaluation of such protocols several metrics have been devised and therefore aim of this thesis is to evaluate selected privacy preserving protocols by application of these metrics.

The rest of the thesis is organized as follows. We describe wireless sensor networks in chapter 2. In chapter 3 we review privacy issues of WSN and describe taxonomy of privacy as introduced in [29]. In chapter 4 we introduced privacy-preserving techniques implemented in practical part of this thesis. Chapter 5 contains description of testing platform, used evaluation metrics. The results for particular privacy-preserving protocols are presented in chapter 6. Finally chapter 7 summarizes results of this work and contains final remarks.

Chapter 2

Wireless sensor network

Wireless sensor network (WSN) is deeply networked system of small autonomous low-cost sensor nodes (motes). These networks may contain from tens to thousands of such sensor nodes, each with very limited processing, storage, sensing and communication abilities. WSN links digital and physical world by measuring a real-world phenomena and converting sensor readings to digital form that can be further processed and possibly acted upon.

2.1 Structure and design

Every wireless sensor network basically contains two different kinds of devices, motes and base stations.

Motes serve as interface between physical and digital world, their purpose is to gather information in demand by means of equipped sensors. Motes can be described as small, independent, very constraint devices, design to be cheap, easy to deploy, possibly equipped with multiple on-board sensors and logically homed to the base station. Sensor nodes are programmed with all the necessary software for their correct operation before their deployment. Their duties depend on the deployment scenario, for example sensor nodes may not only monitor some physical phenomena or track targets, but can also serve as relay points and aggregation points for other motes in matter of data re-transmission to the base station.

The base station is a device in the WSN with more computational, communication, storage and energy resources. It consists basically of radio, for receiving data from the sensor nodes, connected to for example laptop, which process received data. The BS can be viewed as a point in the wireless sensor network where all the data, from all the other motes, are aggregated, therefore it is commonly also referred to as a *sink*. Such device also usually acts as a gateway between motes in the WSN and other systems and networks. It can relay received data further over different medium to others designated devices or networks for further processing. Because the BS is usually only one in the whole network, it is a final aggregation point and therefore also a potential single point of failure for entire WSN.

2.1.1 Hardware platform

Sensor nodes have to operate efficiently in many environments and under various and sometimes rather harsh conditions. The WSN topology often cannot be predicted before deployment and therefore is usually build ad-hoc. These facts predict design needs for properties of the sensor nodes, they should be self-sufficient and able to adapt to current situation, discover neighboring motes, establish communication links, etc. There are already numerous sensor node's platforms and few companies manufacturing them, for example MICAz[8], IRIS[5, 6], TelosB[11, 12] platform and companies like Crossbow[4] or Memsic[7].

Generally, motes consists of computational, communication, power, storage and sensing unit. The computational unit is usually some kind of micro-controller unit (MCU) [24], such as TI MSP430 [9] or Atmel Atmega128L [2]. The communication unit is commonly comprised of a radio frequency transceiver, for example CC2420 [3] or AT86RF230 [1]. Therefore available underlying hardware components are solely dependent on the platform. For example MICAz platform is equipped with the Atmel Atmega128L MCU and the CC2420 RF transceiver. Motes are powered usually by exhaustible batteries and use flash, RAM and EEPROM memory for storage of program code, sensed data or some mote's configuration data. Types and number of equipped sensors varies, commonly available are temperature, humidity, light, acceleration, acoustic or pressure sensors. From this may be obvious that sensor nodes have many constraints starting with the amount of available energy, followed by the communications range, computational power and ending with the amount of available memory. These constraints require effective implementations of applications, which is quite challenging.

2.1.2 Software platform

To ease and simplify software development for the WSN, various operating systems and tools are continuously being developed. To popular operating systems belong TinyOS [19, p.75], programmed in the nesC programming language [23, 10], LiteOS [19, p.85] or Contiki [19, p.80].

Very useful tools to test applications are simulators. TinyOS provides a TOSSIM [28, 14], which is designed to simulate this entire operating system. TOSSIM is very fast simulator capable of simulating hundreds of motes but it does not provide an energy consumption model to simulate the energy requirements of the simulated application. Another interesting simulator is Avrora [35], this simulator is developed by UCLA Compilers Group [15]. It is a simulation and analysis framework, written in Java, for applications written for the AVR micro-controllers. Avrora's framework contains many useful tools for analysis, experimentation and profiling. One of the advantages of this simulator is, as presented in [35], its capability to accurately profile energy consumption of simulated application, which is desired for predicting WSN lifetime before deployment.

The applications themselves can be programmed for example in the nesC programming language. The nesC programming language is an extension to popular C programming language. The nesC is a component-based programming language. Programs are built out of components by *wiring* necessary components to form a whole program. Component behavior is specified by bi-directional interfaces, which define functions implemented by interface's providers (*commands*) as well as functions needed to be implemented by interface's users (*events*). Wiring of the components is done via configurations, special components implemented by assembling (wiring) other components. Implementation of the interface's commands and events is done in the modules. Program may consist of several modules and configurations, which are finally wired in the one top-level configuration. Wiring of the components is static, increasing runtime efficiency and allowing better static analysis of programs.

2.1.3 Communication protocols platform

Because motes not only collect data, from on-board sensors, but in the real applications, they also have to be able to collaborate with neighboring motes in data packet re-transmission. In the WSN, mote-to-mote communication is facilitated by the means of mote's radio transceiver. Use of wireless communication ease the WSN deployment, motes can be thrown out of an airplane, but at the same time requires a use of protocols for an ad-hoc network topology creation, to allow successful delivery of data to the BS. Also WSN may operate on large geographic area making it impossible to every sensor node to be in communication's range of the BS, which necessitate a use of multihop communication scheme and appropriate routing and higher-level transportation protocols to ensure data delivery. Figure 2.1 illustrates two different network communication schemes, on the left is rarely feasible topology in the WSN, where nodes are organized in the star topology, and on the right is multihop communication scheme where nodes are ordered in partially connected mesh topology.

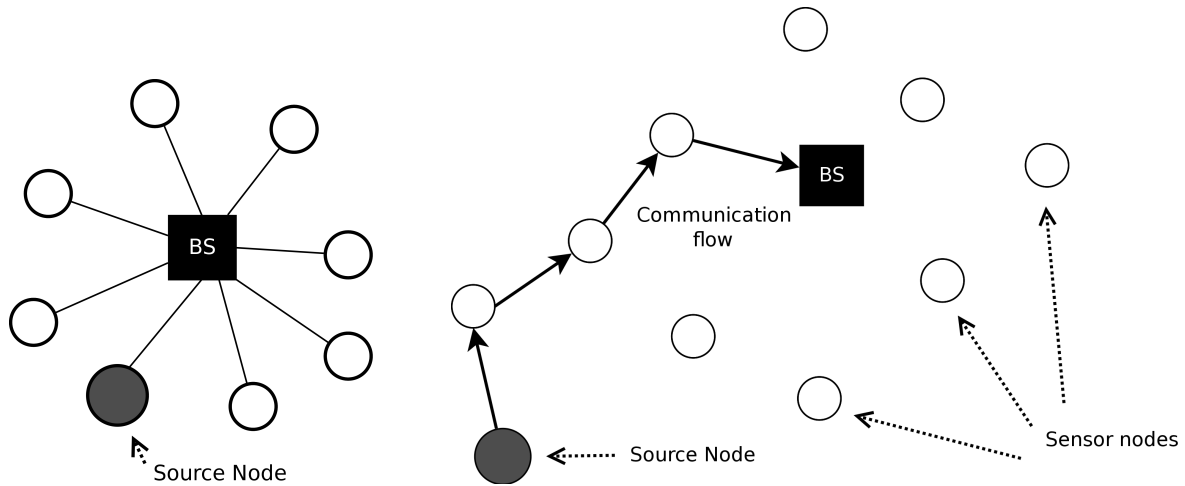


Figure 2.1: Example of single-hop and multi-hop WSN topologies

WSN's protocols stack is similar to ISO/OSI but it has to correspond to specific properties and requirements of the wireless sensor networks. A lot of research was focused on enabling low-power and reliable communication in the WSN as a result are many efficient media-access control (MAC), routing and transportation protocols. While efficient communication in terms of energy consumption and amount of packets is important, there are other issues like security and privacy, which are not addressed by these protocols, but are needed by many applications.

2.2 Applications

Traditional sensor network research was motivated by military applications [18, p. 1257], like ground target tracking or large-scale acoustic surveillance systems. Another traditional applications were in context of high-end application, like radiation detection or seismic activity monitoring. However, the progress in engineering and computer technology development allowed for creation of low cost sensor devices and communication network technologies,

that have influenced many new and potentially useful applications. The list of these applications is remarkable diverse, including :

- **Military applications** – battlefield surveillance, target tracking, damage assessment, attack detection, they all benefit from WSNs structure and properties. Ease of deployment of sensor nodes and ad-hoc topology suites the needs of these applications.
- **Environmental and habitat monitoring applications** – potentially promising area for practical WSN deployment. Deployed WSNs can measure several physical phenomena, like temperature, pressure, humidity, etc. , therefore, can act as warning system for natural catastrophes, like forest fire or earthquake. Another useful way of use of this technology can be for example tracking of endangered species, various habitat monitoring applications [31].
- **Health-care applications** – many health-care applications of the WSN were proposed [17], including monitoring of vital functions of patients, suffering from diseases requiring constant medical attention, monitoring of movement in medical facilities. These applications present considerable issues for privacy preservation of collected information by the WSN which inhibit their utilization.
- **Infrastructure monitoring applications** – similar to environmental and habitat applications, this category includes couple interesting examples. For example WSNs can be used to protect water, oil or gas pipelines, electrical grids from unauthorized intruders or help with their management. Another way to apply WSNs is in traffic control to prevent congestion by monitoring various aspects of traffic.
- **Industrial applications** – machine maintenance, control of process of production and better management of resources. Sensor nodes can measure and monitor different conditions affecting production and in case of danger or problem warn or stop the process.
- **Home applications** – WSNs can find their place even in our common life. In smart homes they provide way of automation different tasks. Sensor nodes could be used to monitor home environment and control unit would act accordingly to events received from these sensor nodes, for example control heating, lights or electronics.

Chapter 3

Privacy-preservation in wireless sensor networks

Inherent features of WSNs and their applications raise security and privacy concerns. The WSN may often operate in uncontrollable environment, where an adversary can capture, destroy or deploy its own sensor nodes. As a result, the adversary can compromise sensor node and retrieve its private keys used for secure communication, which would allow him to decrypt the communication. Next, all the gathered information are transmitted through several nodes, across freely accessible physical medium, air. The adversary can apply traffic-analysis techniques to infer valuable information from eavesdropped communication. On top of that, the lack of node's resources make privacy-preservation a quite challenging problem. A lot of research has been done concerning privacy-preservation in variety of fields related to WSN like wired and wireless networking, databases and data mining[29]. Following game, called panda-hunter game[33] presents unique challenges in wireless sensor networks and the need for efficient privacy-preserving techniques. This game can be used to model and assess effectiveness of privacy-preserving techniques.

3.1 Panda-Hunter game

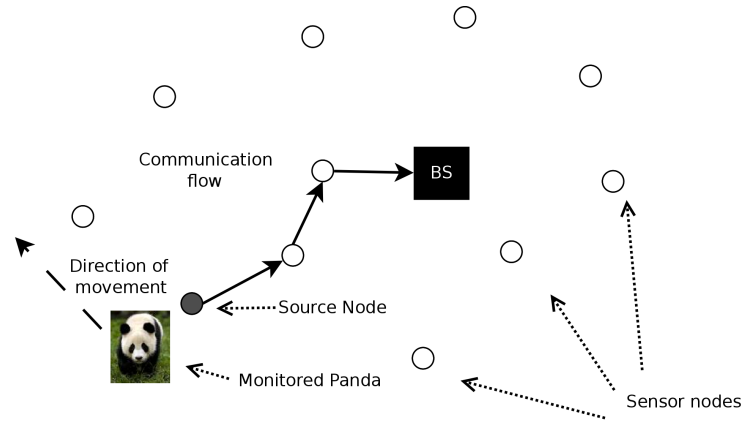


Figure 3.1: Illustration of the WSN communication flow in the panda-hunter game

This game consists of deployed wireless sensor network, capable of detecting pandas and two participating parties, network's operator in defender's role and a hunter in the role of the adversary. Sensor nodes report observations of the panda to the BS periodically. The defender's main concern is panda's safety. Hunter's goal is to determine panda's location by eavesdropping WSN's communication and back-tracing the routing path of messages until it reaches the source node, which initiated the communication. If the messages sent between

sensor nodes, were only encrypted and no privacy-cautious routing techniques were used, hunter would easily trace the source of this transmission to the originating mote, which would lead him to the panda. However if the communication path from the source node to the base station has been protected by using privacy-preserving technique, panda would be safe. The game ends if either the hunter captures the panda or the time for tracking expires.

Additionally the hunter does not interfere with motes communication and posses more powerful devices and he is not constraint by the lack of resources such as amount of energy or memory and also we can assume that the hunter knows the location of the BS and various techniques used to protect the panda.

3.2 Adversary models

From defender's standpoint there are several types of adversaries. They can be divided into two main groups, internal and external. These can be thereafter divided to passive and active or local and global eavesdroppers depending on their collaboration in the network operation, monitoring capabilities, amount of resources etc.

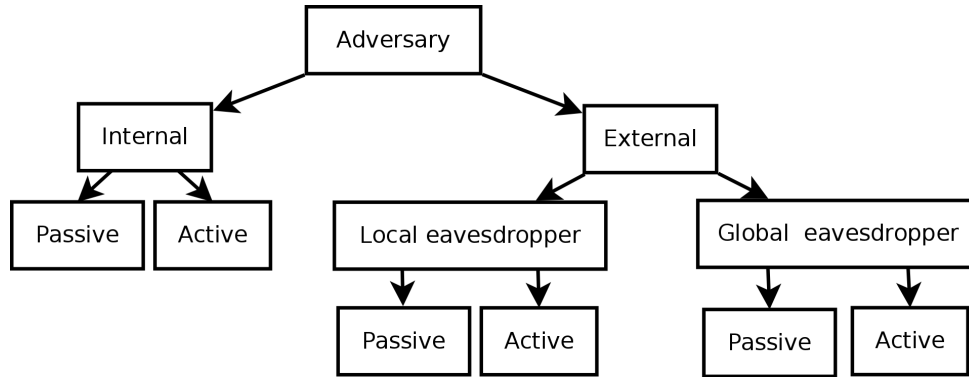


Figure 3.2: Taxonomy of adversary models in WSNs

3.2.1 Internal adversary

This adversary is legitimate member of defended network. Internal adversary can have multiple abilities, can posses decryption keys used by motes in the network or could have compromised, possibly one or more motes itself. Therefore captured sensor node, compromised by malicious entity is also considered to be an internal adversary.

3.2.2 External adversary

Opposite to internal adversary, does not posses precious resources of defended network but can deploy his own sensor network for eavesdropping communication in network of interest. This adversary can be further addressed as local or global eavesdropper where each of these two can also be considered a passive or active adversary.

3.2.3 Local eavesdropper

Stands for adversary with limited monitoring capabilities. Usually this kind of adversary is capable of monitoring and applying flow analysis only on some part of the sensor net-

work. Because of this counterfeiting this adversary is easier and there already exist several effective protocols. These protocols exploit disability to see traffic pattern of whole network communication and therefore detect hot spots in the network. Disrupting network flow by routing packets through multiple paths is effective strategy in ensuring privacy against this adversary.

3.2.4 Global eavesdropper

Also referred to as strong adversary is type of adversary capable of capturing virtually all communication in the wireless sensor network in real time. Usually these are highly motivated and well financed individuals able to deploy own network of motes to cover the same area as defender.

3.2.5 Passive adversary

In this category are adversaries that obtain information from the network only by passively monitoring communication from which they infer as much information as possible.

3.2.6 Active adversary

Adversary is considered to be active if he is taking proactive steps towards successful obtaining of desired information. This is opposite to the previous category. Active adversary can modify eavesdropped communication, execute various types of attacks like man in the middle attack, jamming of communication etc.

3.3 Taxonomy of privacy in WSN

Figure 3.3 depicts the privacy taxonomy for WSNs. From this figure can be seen that there are two main types of privacy concerns, data-oriented and context-oriented.

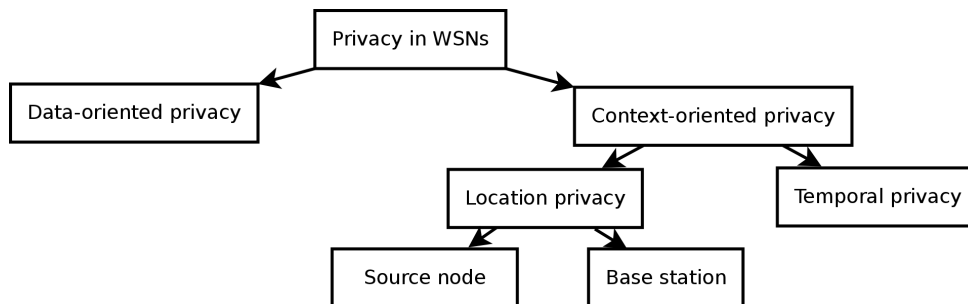


Figure 3.3: Taxonomy of privacy in WSN according to [29]

3.3.1 Data-oriented privacy

Privacy-preserving techniques for the data-oriented privacy focus on protection of data-content of sensed data by the sensor nodes as well as queries posted to the wireless sensor network by its users. Data-content privacy can be protected by using traditional cryptographic techniques. Data-content is encrypted and authenticated by sensor nodes. While

traditional cryptographic techniques are effective against external adversary they may not be sufficient against internal adversary [29].

3.3.2 Context-oriented privacy

Protection of context-oriented privacy, as depicted by figure 3.3, is focused on protecting either location or temporal privacy in wireless sensor network. Temporal privacy [25] concerns timing information such as time of data creation at source node, time of transmission, etc. Knowledge of such information for example enables, in target tracking applications, movement prediction and therefore violates privacy of monitored object. Location privacy [32, 33, 26] rises with special parts of the WSN such as source nodes or base stations. The knowledge of the location of these key nodes enables the adversary to destroy such nodes, in case of the base station it disables the entire WSN [20], or to conclude nature of data without the need of determining data-content. Context-oriented privacy can be compromised by both external or internal adversary, however the context-oriented privacy-preserving techniques evaluated in this thesis are focused on the external adversary only. As shown in the figure 3.2 external adversary can be either local or global adversary, which reflects number of available privacy-preserving techniques to protect contextual information.

3.4 Privacy attacks

The wireless sensor networks are susceptible to different types of attacks[22, 34, 36]. The privacy in the WSN can be violated mainly by attacks based on traffic analysis [29, 20, 21].

3.4.1 Traffic analysis

Traditional cryptographic techniques can be applied to assure data-content confidentiality. Nonetheless by analyzing communication traffic and its patterns in monitored network, the adversary may still learn valuable information about the network and monitored objects. Traffic analysis is a passive type of attack that attempts to infer communication patterns from eavesdropped packets. The traffic-analysis attacks are generally executed in three ways [30]:

- **Rate-monitoring attack** – this kind of attack is based on assumption that amount of traffic generated by sensor nodes decreases with their distance from base station. The adversary is tracking and moving towards the sensor nodes with higher communication intensity.
- **Packet tracing attack** – the adversary observes sending time of correlative data packets between neighboring nodes in the WSN and traces the packet hop-by-hop until it reaches either base station or source node.
- **Identity analysis attack** – in this attack the adversary is attempting to infer relations between particular sensor nodes by analyzing source and destination addresses stored in packet headers.

Chapter 4

Privacy preserving protocols

In this chapter are described privacy preserving protocols implemented and evaluated in practical part of this thesis. The described and implemented protocols are designed to protect location privacy against the global eavesdropper. These protocols are periodic collection protocol and source simulation protocol, proposed in [32].

4.1 Periodic collection protocol

Periodic collection protocol introduced in [32] is one of the first protocols designed to protect location privacy against the adversary as powerful as global eavesdropper. This protocol approach is very simple and straightforward. Its idea is based on flattening communication patterns of all motes in the WSN to prevent adversary from deducing information about location of source node. Because if every mote in the network has roughly the same communication pattern it becomes harder for adversary to trace the desired events in the WSN.

4.1.1 Protocol description

In periodic collection protocol each mote in the WSN has timer with predefined repetition period and FIFO queue for storing received packets with arbitrary but fixed size. Timer period and queue size is the same for all motes. In every period mote broadcasts data packet. Transmitted packet can contain either real sensed data or dummy data. Packets with dummy data (dummy packets) are differentiate from packets containing real sensed data (real packets) in reception process at receiving mote. Every packet payload is assumed to be encrypted before transmission with unique mote-to-mote encryption key. Dummy packets are filtered through packet authentication. These packets do not authenticate correctly at receiving node and are discarded. Correctly authenticated packets are en-queued to mote FIFO queue and in the next period re-transmitted closer towards base station.

Because every mote will always transmit some packet and every packet will be encrypted adversary will not be able to distinguish between them. This protocol therefore provides best possible privacy. Gained privacy is however exchanged for increased power consumption and latency between time of an event and actual reception of packet, reporting this event at the BS. Increase of power consumption is due to periodic communication between motes even if nothing has happened. Because it takes several periods to propagate packet from source mote to base station the freshness of information is reduced. Obviously, range of the latency is determined by period length and queue size. Shorter periods increase power consumption but message latency can be reduce. Small queue size also reduces latency but can effect reliability. If number of received real packets exceeds size of queue, packets are dropped, and depending on implementation, may not be re-transmitted again. On the other hand large queue can prevent dropping of received packets but it may also increase amount

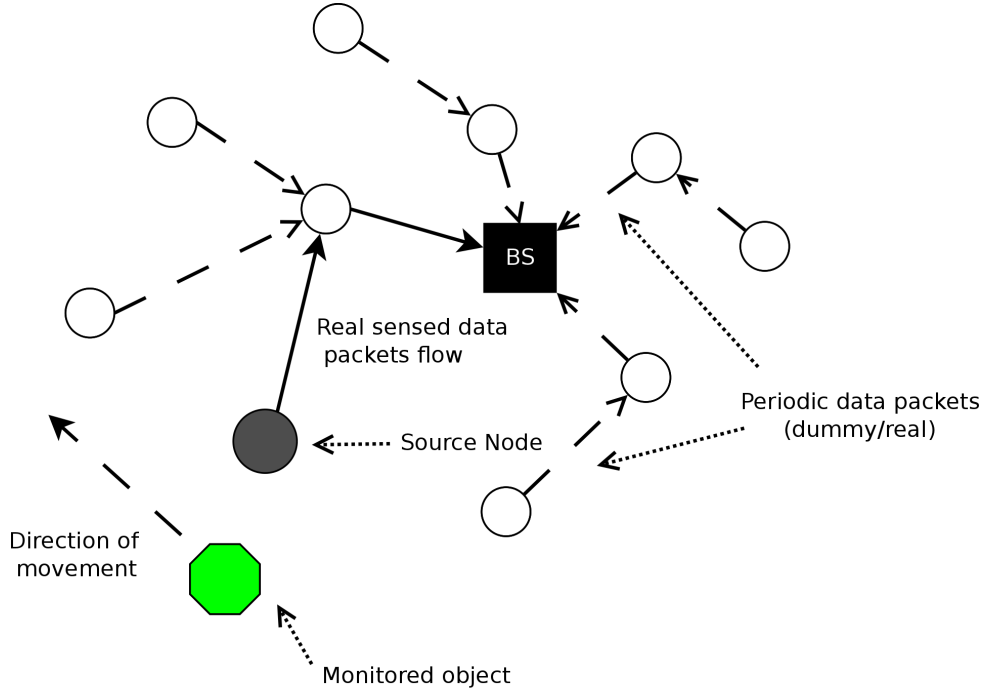


Figure 4.1: Periodic collection protocol traffic pattern illustration

of time before packet can be relayed further. However these values are application dependent and have to be set to suite the needs of the application. Figure 4.1 depicts communication pattern of the WSN if the periodic collection protocol is applied.

4.2 Source simulation protocol

Second protocol introduced in [32] is source simulation protocol. Source simulation protocol makes trade-off between power requirements and level of provided privacy. This is accomplished by reducing the number of candidate traces in the network.

4.2.1 Protocol description

The source simulation protocol has two phases, pre-deployment phase and after-deployment phase. Before deployment of the WSN a subset of all sensor nodes is chosen. Each such sensor node is programmed with unique virtual token, identified by unique ID. After deployment of the WSN source simulation protocol works in rounds. In every round the motes possessing the token (token nodes) will emit signal which mimics signal emitted by monitored object. Afterwards token node decides which of its neighbors, including itself, is going to simulate source node in the next round, based on a behavior model of a real monitored object. Token is then passed to chosen mote. Idea behind this process is to generate multiple traces of the events in the WSN, to increase the safety period of the real events but reducing amount of consumed power and necessary traffic.

Source simulation protocol assumes that defender's and adversary's knowledge about

the behavior of the monitored object does not significantly differ. Therefore accurate behavior model based on the knowledge is key part to correct operation.

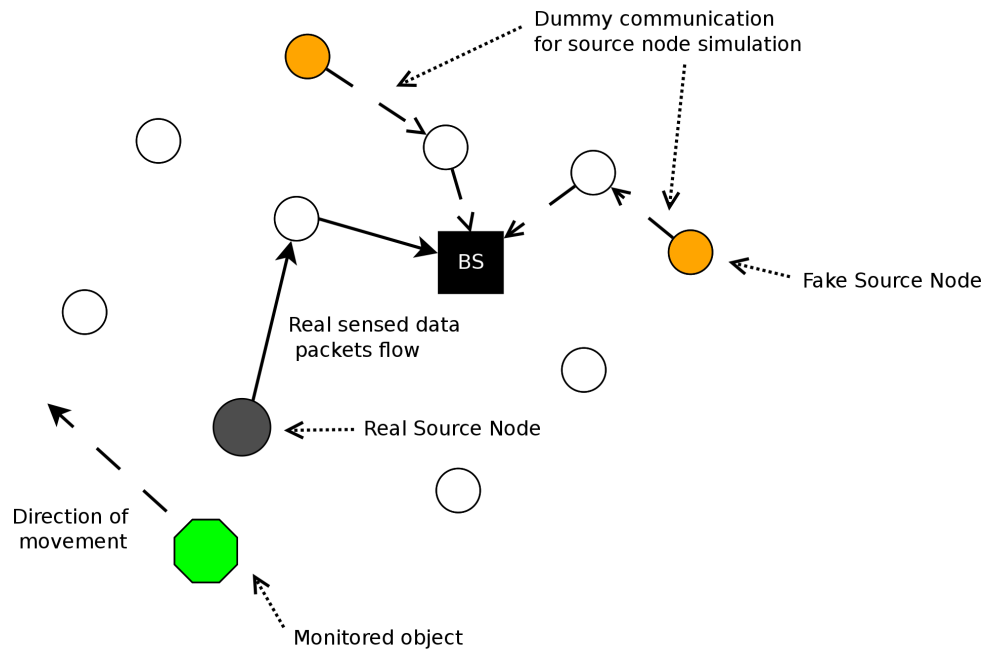


Figure 4.2: Source simulation protocol traffic pattern illustration

Chapter 5

Evaluation

5.1 Metrics

Evaluation of the protocols presented in section 4 is done by using following metrics defined in [27]. They evaluate various performance aspects of protocols, each important for feasibility of privacy protocols in real applications. Described metrics will follow formal definition in [27], where C is a set of $c_1, \dots, c_n$ of $n \in \mathbb{N}$ sensor nodes in WSN.

5.1.1 Performance metrics

- **Energy consumption** in sensor networks is a crucial design factor, because sensors are commonly battery driven. For developers it is important to evaluate the power consumption of applications accurately, since the choice of algorithms heavily influences energy consumption. Once nodes are deployed, it may be challenging or impossible to change batteries in the field. Therefore poor lifetime estimates may cause high costs or even render a sensor network useless before its purpose is fulfilled. First of three metrics for energy consumption expresses total amount of energy consumed by network.

$$m_1 = \sum_{i=0}^n F(comm_i, comp_i) \quad (5.1)$$

Where function F is defined as addition on real numbers, $comm_i$ and $comp_i$ are real numbers representing amount of energy spent by communication and computational unit. Following energy consumption metric is designed to visualize energy map of entire network, its output is a list of values, where each value is amount of consumed energy by particular node in the WSN expressed as output of function F .

$$m_2 = [F(comm_1, comp_1), \dots, F(comm_n, comp_n)] \quad (5.2)$$

Finally this energy consumption metric determines lifetime of the wireless sensors network in seconds before percentage p of sensor nodes depletes their battery.

$$m_3 = T_c(p) \quad (5.3)$$

- **Memory usage** of sensor nodes is another important design factor. Sensor nodes have limited memory size which limits amount of data particular sensor node can store. To view maximum memory requirements, following metric is presented.

$$m_4 = \max\{mem_1, \dots, mem_n\} \quad (5.4)$$

This metric takes information about memory usage of a sensor node during time interval T and returns maximum of them.

- **Communication cost** is amount of additional traffic needed to transmit message from source to base station. Network traffic is comprised of types of data packets, real data collected by sensor motes and support traffic. To support traffic belong cover traffic used by privacy preserving protocols, management traffic used to reprogram network to fit the changing needs etc. For application, in the case of this thesis, privacy preserving protocols, to be feasible under all the constraints there should be chosen careful trade-off between amount additional cover traffic and privacy. First metric express overall number of bytes particular mote has sent.

$$m_5 = \sum_{i=1}^n numSent_i \quad (5.5)$$

Next metric estimates summation of received and sent bytes.

$$m_6 = \sum_{i=1}^n (numSent_i + numRev_i) \quad (5.6)$$

As convenience for easier presentation, last metric in this group measures number of packets sent by mote.

$$m_7 = \sum_{i=1}^n numSentp_i \quad (5.7)$$

- **Message latency** influences freshness of collected information by the WSN. Each message is encapsulated into data packet and sent towards base station. This data packet is received at different time as it was sent. The difference between this two values reveals delay between transmission from source mote and reception at the BS mote. M is number of all messages. Each deployment scenario has different needs for latency values therefore by this metric is possible to determine suitability of chosen protocol for particular application and also find potential bottlenecks in network communication leading to improvement in communication effectiveness. First of two metrics used reveals average delay between message creation and reception at the BS.

$$m_8 = \frac{1}{M} \sum_{i=1}^M t_{m_i} \quad (5.8)$$

- **Availability** of collected information is crucial for every application. In ideal call all information should be available at any time during network's lifetime. However many deployment scenarios are far from ideal. Therefore this metric express percentage value of information availability measuring number of events received by BS within specified time $t_{availability}$ and number of all occurred events.

$$m_{10} = 100 \frac{numEventsBS}{numEventsAll} \quad (5.9)$$

- **Reliability** is always a concern in any kind of network. Highly reliable networks therefore have to be robust. WSN structure greatly supports robustness. However messages

can still become lost, dropped or corrupted due to wireless communication medium for various reasons. This metric express lost ratio of the network during time period T . $numAllM$ is a number of messages that were initiated during time period T . $numLostM$ is a number of messages lost during time period T , meaning, messages initiated but not received by the BS within specified time $t_{reliability}$.

$$m_{11} = \frac{numLostM}{numAllM} \quad (5.10)$$

5.2 Testing platform

For the purposes of protocols evaluation was chosen MICAz [8] node platform and TinyOS [13], operating system for wireless sensor nodes. Privacy-preserving protocols described in sections 4.1 and 4.2 were implemented in nesC.

Testing of protocols was conducted via protocol simulation in TOSSIM [14] and Avrora [15] simulators with multiple network topologies and different number of nodes. Data extracted from these simulations were analyzed by metrics defined in section 5.1. Simulations were conducted with topology configurations containing up to 100 sensor nodes. Nodes were distributed either in random or grid fashion.

Protocols implementation includes except privacy-preserving protocols also a simple routing protocol, to enable end-to-end communication. On top of this are build testing applications. Routing protocol module contains simple structure representing routing table. This structure holds three unsigned integers. Two of these integers are 16-bit network addresses, the base station and a *parent node*. The *parent node* is the mote closer to the BS in routing tree. Routing protocol module also has methods for accessing and modifying its routing table. BS initiates building of WSN routing topology by sending *beacon packet*. Beacon packet mainly contains the BS address, distance to the BS and address of sending node. This packet is relayed by all motes in the WSN. Each mote updates two values, distance to the BS and address of sending node. In periodic collection protocol each mote accepts only the first received beacon, every other is discarded. In source simulation protocol several beacons are accepted. Source simulation protocol uses slightly altered version of the routing protocol module, where routing table can store predetermined amount of parent node addresses. Ultimately choice of routing protocol does not affect results of evaluated protocols.

Chapter 6

Results

In this chapter are presented results of our simulations of implemented privacy-preserving protocols.

Simulation results for both protocols were influenced by two main aspects, first length of FIFO queue used to store data packets and second the timer period length. In addition in source simulation protocol, number of token nodes and behavior model affected the results.

6.1 Energy consumption

Figure 6.1 present relation between the amount of consumed energy by all sensor nodes in the WSN and the duration of simulations. The periodic collection protocol consumption turns to be greater in the longer WSN operation. However in the short-term there is minimal difference between these two protocols.

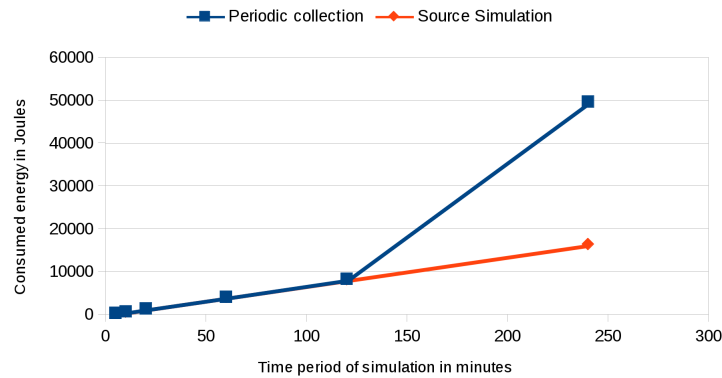


Figure 6.1: Total energy consumption of the WSN

Figure 6.2 depicts example of the energy consumption of each sensor node running periodic collection protocol during the single simulation, as seen all the sensor nodes consumed approximately the same amount of energy during the simulation.

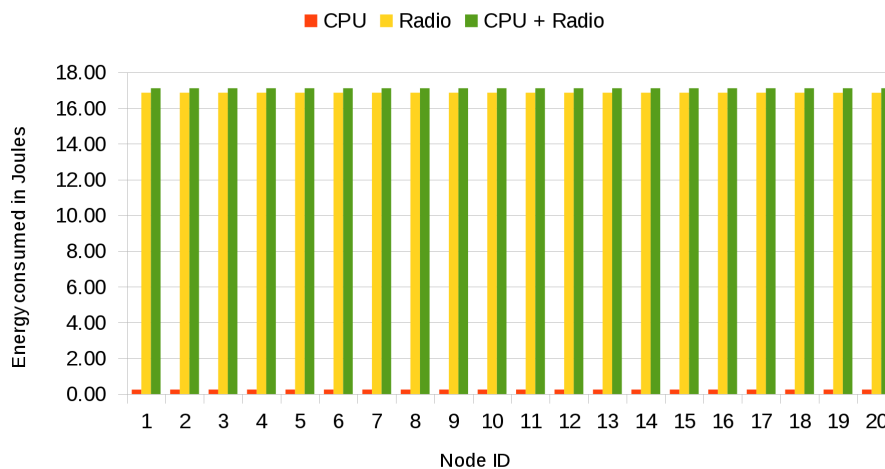


Figure 6.2: Energy map of the Periodic collection protocol

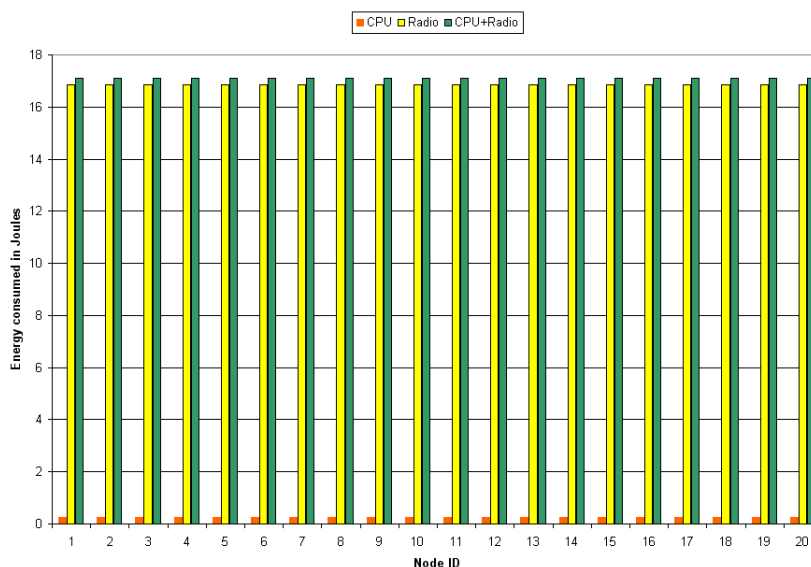


Figure 6.3: Energy map of the Source simulation protocol

This is due to the fact that every sensor node in the WSN periodically transmits some data packet and so sensor nodes are frequently using their radios. From this may be inferred direct relation between energy consumption and communication cost of the protocol. Also it can be seen that impact of the CPU energy consumption is minimal in comparison with radio energy consumption. It is important to keep in mind that these values are mainly affected by the length of timer's period. Shorter delays between two consequent transmission increase amount of energy consumed during time period. To apply metric m_8 to measure a lifetime of the WSN we have to distinguish importance of sensor nodes. The lifetime of the WSN is

dependent on the lifetime of the sensor nodes in communications range of the BS. Because these nodes provide link between the rest of the WSN and the BS, their failure due to energy source depletion results in disconnection of the BS from the rest of the WSN. From figure 6.2 is obvious that lifetime of the WSN using periodic collection protocol is the same as lifetime of any of the sensor nodes, because all sensor nodes will deplete their power sources approximately at the same time. Lifetime of the WSN is therefore affected by rate of radio communication.

6.2 Communication cost

Generally communication cost is related to communication rate, therefore shorter delays between two subsequent transmission create more communication overhead during time interval. The periodic collection protocol communication cost is high. For every real message needed to be transmitted to the BS, each sensor node which is not in the routing path from the source node to the BS potentially creates cover dummy traffic, to protect location of the source node. By potentially we mean that in case of multiple monitored objects there can be more than one real message in the WSN.

For source simulation protocol the situation is better because the amount of traffic is dependent on number of token nodes simulating the real source node and of course on the number of monitored objects. Therefore only token nodes create cover traffic, which reduce total communication cost. However the amount of received packets can be still high, this is due to operation of the sensor node. If the sensor nodes that not participate in the communication, they are not attempting to send real sensed data or do not possess token, are not turned off, the amount of consumed energy is the same as if they were actively communicating, because sensor node's radio consumes most of the energy even if the sensor node is only listening to the communication of neighboring nodes.

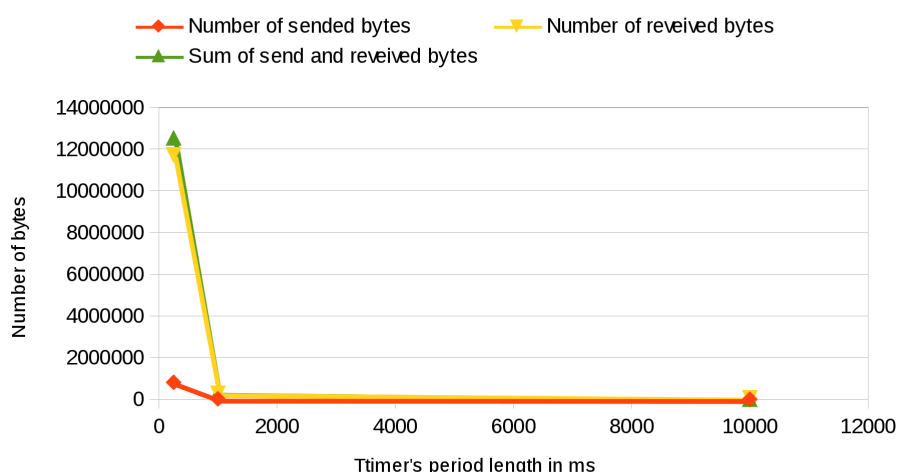


Figure 6.4: Periodic collection communication cost in bytes

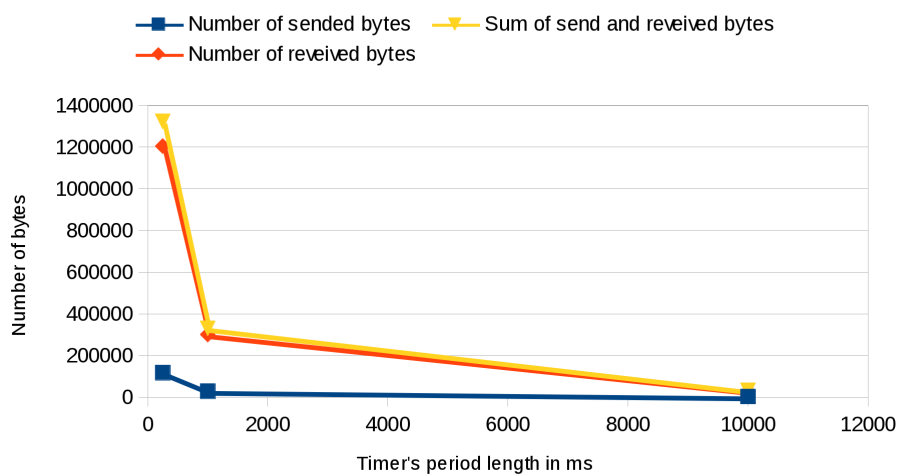


Figure 6.5: Source simulation communication cost in bytes

Figure 6.5 shows results for metrics m_5 and m_6 with respect to length of the timers period used to simulate rounds of the protocols. As could be expected the amount is decreasing with longer timer's periods. First of the two graphs presents communication cost of the periodic collection protocol and the second graph is presenting results for source simulation protocol. These graphs again shows efficiency of source simulation protocol, its communication cost is almost 10-times smaller than in periodic collection protocol. This is again due to the fact that only portion of the WSN is communicating in each protocol round and also it is important to mention, that dummy is created only for real packets and not every-time when sensor node has nothing to send. Figure 6.6 shows for convenience results from metric m_7 .

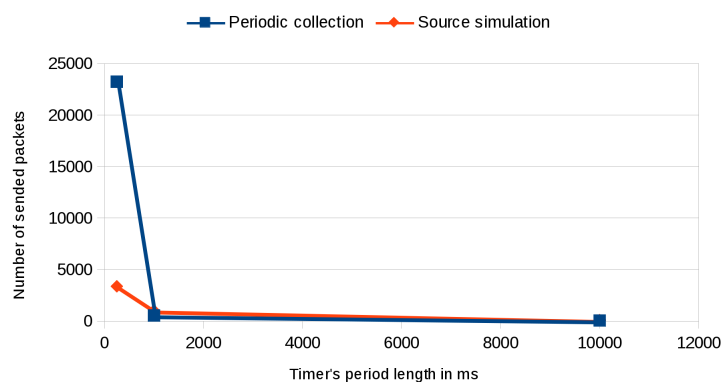


Figure 6.6: Communication cost in packets

6.3 Message latency

Time delay between a message creation by the source node and reception by the BS is proportional to the distance from the BS and the communication rate, meaning, latency is effected by the number of hops needed to transmit the message from the source node to the BS. However this gives only lower limit for the latency. Message can be further delayed if queue of an intermediary mote is not empty. In this situation, at first all messages that were received earlier would be transmitted, thus increasing latency. Figure 6.3 depicts influence of queue length on the message latency in the source simulation protocol. From this figure is obvious that larger queues cause increase in latency. As was said above this is due to fact that multiple message can arrive and are transmitted one-by-one in every round.

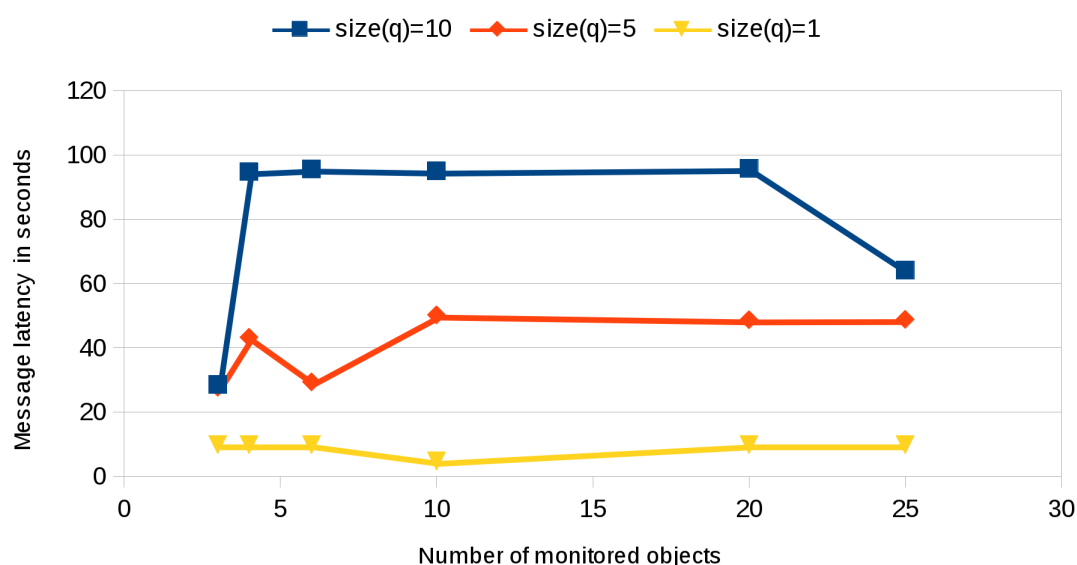


Figure 6.7: Message latency of the source simulation protocol

Like figure above next figure presents impact of the queue size on the message latency for periodic collection protocol.

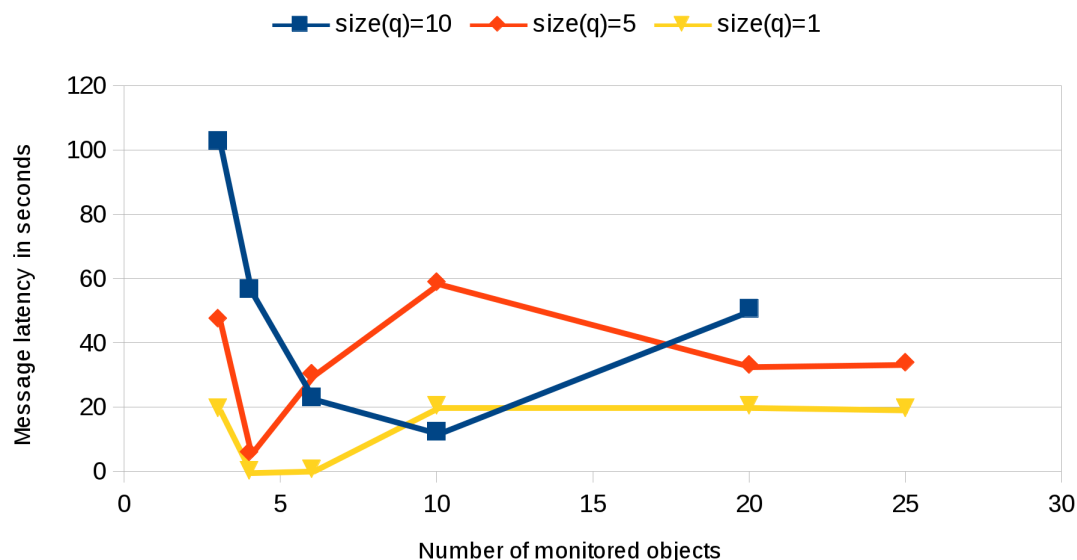


Figure 6.8: Message latency of the periodic collection protocol

6.4 Memory usage

Memory usage of both protocols depended on the communication rate of data packets with a real payload and queue size, because only real packets were stored in the queue. Figure 6.9 shows estimations of the protocol's memory requirements computed by the nesC compiler. Values in this table were affected mainly by the queue size because queue for storing messages requires the most memory.

Queue size	Compiler assumption of memory requirements in bytes			
	Periodic collection		Source simulation	
	RAM	ROM	RAM	ROM
1	13450	428	13680	450
5	13450	492	13680	530
20	13450	732	13680	890

Figure 6.9: Memory requirements assumption

To measure maximum amount of memory used by each protocol, multiple simulations were conducted and the data retrieved from the Avora simulator after each simulation are depicted in the figure 6.10. The source simulation protocol uses slightly less memory because sensor nodes not participate in communication did not store any packets in their queues. However the difference is not significant. Also it needs to be said that results for single sensor node ranged from 133 bytes to 237 bytes for periodic collection and from 88 bytes

to 199 bytes for source simulation protocol during simulations. These results depended on number of real and dummy messages, queue size and also on timers period length.

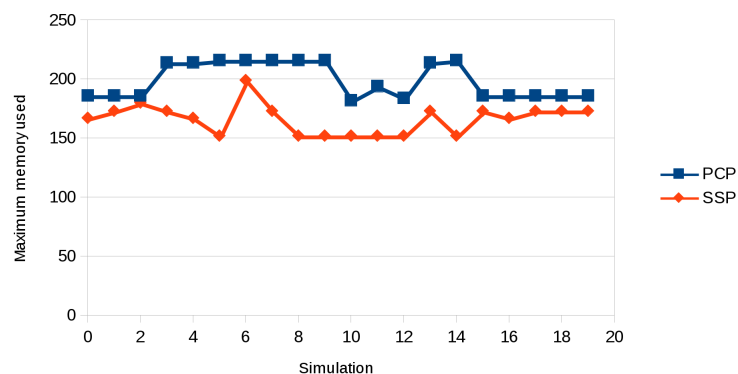


Figure 6.10: Maximum memory usage of protocols

6.5 Reliability

Reliability of data delivery can be affected by many aspects. Value of latency or queue size affect the reliability results. Reduced reliability occurs when latency of messages is higher than desired by application or when queue size is smaller than needed, resulting in dropping packets. Particularly dropping of packets is dangerous because they do not have to be transmitted again.

Queue size	Privacy preserving protocol	Lost ratio (average)
10	Source simulation protocol	0.0509398019
10	Periodic collection protocol	0.0731757384
5	Source simulation protocol	0.0272299969
5	Periodic collection protocol	0.0426147589
1	Source simulation protocol	0.0183213805
1	Periodic collection protocol	0.0376344086

Figure 6.11: Reliability of privacy preserving techniques

In figure 6.11 are presented results for lost ratio of particular protocols in relation to queue size. As can be seen lost ration of the periodic collection protocol is slightly higher than lost ration of the source simulation protocol with the same queue size.

6.6 Availability

Queue size	Privacy preserving protocol	Total number of events detected by WSN	Number of reports received by the BS	Availability
10	Source simulation protocol	84	79	94.04761905
10	Periodic collection protocol	85	81	95.29411765
5	Source simulation protocol	86	82	95.34883721
5	Periodic collection protocol	87	84	96.55172414
1	Source simulation protocol	89	85	95.50561798
1	Periodic collection protocol	89	86	96.62921348

Figure 6.12: Availability of privacy preserving techniques

From our simulations results that periodic collection and source simulation protocols provide good availability. Results in the figure 6.12 are based on the data used for the metric m_{11} and were mainly affected by the queue size.

All the results presented in this section confirm what was expected. Periodic collection protocol is very powerful in providing privacy in the wireless sensor network, however his disadvantages are communication cost and power consumption. Its need to periodically communicate drains much of the precious resources from the sensor node. On the other hand source simulation provides good trade-off, but his shortcoming is the need of accurate behavior model. Without accurate model the communication pattern can be easily analyzed leading to violating of the privacy.

Chapter 7

Conclusion

Aim of this thesis was to study privacy protection issues in wireless sensor networks. Consequently implement selected privacy-preserving techniques for the wireless sensor networks and their evaluation by selected metrics.

The first chapter is focused on introduction to the field of wireless sensor networks, in the chapter are described wireless sensor networks in general, their advantages and disadvantages as well as their impact on the privacy.

The second chapter contains description of hardware and software platform in wireless sensor networks with their constraints and shows the requirements for communication stack in wireless sensor networks. Also in this chapter there are summarized different areas of possible application for the WSN.

In the third chapter there are presented privacy issues in wireless sensor networks by means of the Panda-Hunter game, followed by taxonomy of adversaries and privacy. At the end of this chapter are described methods used to violate privacy in the WSN.

Chapter four for presents privacy-preserving techniques for global eavesdropper with detailed description of their logic and properties. At the end of this chapter there are some implementation remarks.

In the fifth chapter we present selected performance metrics for evaluation of implemented protocols, in matter of power consumption, communication cost, memory usage, latency, reliability and availability. Final and the most important chapter presents simulation results of protocols from chapter 4 and explains their meaning and influence on protocol applicability. Hopefully we discussed all the possibilities that can influence particular results and explained their relevance.

The result of this thesis are, two implemented privacy-preserving mechanisms for the TinyOS operating system. Constraints of the WSN are challenging and therefore in effective implementation of privacy-preserving mechanisms have to be considered many aspects of the wireless sensor networks as well as the application requirements. Not every application can choose from all the available privacy-preserving mechanisms, therefore such decision should be made carefully to prevent disasters, like ineffective protection of privacy or the WSN malfunction before its intended lifetime. As shown in this thesis, simulations can be very useful in predicting behavior of application and help discover potential problems, enhance effectiveness and help in decision making.

However there are still many open problems in the field of wireless sensor networks and because as discussed in chapter three, privacy-preservation is studied across different fields in computer science and from these can easily arise new, better and more effective privacy-preserving mechanisms and evaluation techniques for better assessment of privacy-presentation mechanisms and allow for wide-spread deployment of this technology.

Bibliography

- [1] AT86RF230 Datasheet [online]. <http://www.atmel.com/Images/doc5131.pdf>. Accessed: 20.12.2012.
- [2] Atmel Atmega128L Datasheet [online]. <http://www.atmel.com/Images/doc2467.pdf>. Accessed: 10.5.2012.
- [3] CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver Datasheet [online]. <http://www.ti.com/lit/ds/symlink/cc2420.pdf>. Accessed: 10.5.2012.
- [4] Crossbow Technology, Inc. [online]. <http://bullseye.xbow.com:81/Home/wHomePage.aspx>. Accessed: 27.12.2012.
- [5] IRIS Datasheet [online]. http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/IRIS_Datasheet.pdf. Accessed: 20.12.2012.
- [6] IRIS Datasheet [online]. <http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=135%3Airis>. Accessed: 27.12.2012.
- [7] Memsic, Inc. [online]. <http://www.memsic.com/>. Accessed: 27.12.2012.
- [8] MICAz Datasheet [online]. http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICAz_Datasheet.pdf. Accessed: 10.6.2012.
- [9] MSP430 Datasheet [online]. <http://www.ti.com/lit/ds/symlink/msp430f1611.pdf>. Accessed: 10.5.2012.
- [10] nesC [online]. <http://nesc.sourceforge.net/>. Accessed: 10.2.2012.
- [11] TelosB Datasheet [online]. http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf. Accessed: 27.12.2012.
- [12] TelosB Datasheet [online]. <http://www.memsic.com/support/documentation/wireless-sensor-networks/category/7-datasheets.html?download=152%3Atelosb>. Accessed: 27.12.2012.
- [13] TinyOS [online]. <http://www.tinyos.net/>. Accessed: 20.12.2012.
- [14] TOSSIM [online]. <http://docs.tinyos.net/tinywiki/index.php/TOSSIM>. Accessed: 27.12.2012.
- [15] UCLA Compilers Group: Avrora [online]. <http://compilers.cs.ucla.edu/avrora/>. Accessed: 10.6.2012.

-
- [16] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks (Amsterdam, Netherlands: 1999)*, 38(4):393–422, 2002.
 - [17] Hande Alemdar and Cem Ersoy. Wireless sensor networks for healthcare: A survey. *Computer Networks*, 54(15):2688–2710, 2010.
 - [18] Chee-Yee Chong and S.P. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, Aug. 2003.
 - [19] Waltenegus Dargie and Christian Poellabauer. *Fundamentals of wireless sensor networks: Theory and Practice*. Wiley Series on Wireless Communications and Mobile Computing . Wiley, John & Sons, Incorporated, 1st edition, September 2010.
 - [20] Jing Deng, Richard Han, and Shivakant Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies For Wireless Sensor Networks. In *DSN*, pages 637–. IEEE Computer Society, 2004.
 - [21] Jing Deng, Richard Han, and Shivakant Mishra. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. *Pervasive Mob. Comput.*, 2(2):159–186, April 2006.
 - [22] Shi E. and Perrig A. Designing secure sensor networks. *Wireless Communications, IEEE*, 11(6):38–43, Dec 2004.
 - [23] David Gay, Philip Levis, Robert von Behren, Matt Welsh, Eric Brewer, and David Culler. The nesC language: A holistic approach to networked embedded systems. In *Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation*, pages 1–11. ACM Press, 2003.
 - [24] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei. Survey of Hardware Systems for Wireless Sensor Networks. *J. Low Power Electronics*, 4(1):11–20, 2008.
 - [25] P. Kamat, Wenyan Xu, W. Trappe, and Yanyong Zhang. Temporal Privacy in Wireless Sensor Networks. In *Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on*, volume 5, pages 28:1–28:24, New York, NY, USA, November 2009. ACM.
 - [26] Pandurang Kamat, Yanyong Zhang, Wade Trappe, and Celal Ozturk. Enhancing Source-Location Privacy in Sensor Network Routing. In *ICDCS*, pages 599–608. IEEE Computer Society, 2005.
 - [27] Jiří Kůr, Václav Matyáš, Andriy Stetsko, and Roman Žilka. Metrics for privacy mechanism evaluation. Internal technical report, Faculty of Informatics, Masaryk University, 2011.
 - [28] Philip Levis, Nelson Lee, Matt Welsh, and David E. Culler. TOSSIM: accurate and scalable simulation of entire tinyOS applications. In Ian F. Akyildiz, Deborah Estrin, David E. Culler, and Mani B. Srivastava, editors, *SenSys*, pages 126–137. ACM, 2003.
 - [29] Na Li, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Netw.*, 7(8):1501–1514, November 2009.

-
- [30] Xi Luo, Xu Ji, and Myong-Soon Park. Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks. In *Information Science and Applications (ICISA), 2010 International Conference on*, pages 1–6, april 2010.
 - [31] Alan M. Mainwaring, David E. Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In Cauligi S. Raghavendra and Krishna M. Sivalingam, editors, *WSNA*, pages 88–97. ACM, 2002.
 - [32] Kiran Mehta, Donggang Liu, and Matthew Wright. Location Privacy in Sensor Networks Against a Global Eavesdropper. In *ICNP*, pages 314–323. IEEE, 2007.
 - [33] Celal Ozturk, Yanyong Zhang, and Wade Trappe. Source-location privacy in energy-constrained sensor network routing. In Sanjeev Setia and Vipin Swarup, editors, *SASN*, pages 88–93. ACM, 2004.
 - [34] Jaydip Sen. A Survey on Wireless Sensor Network Security. *IJCNIS*, 1(2), 2009.
 - [35] Ben L. Titzer, Daniel K. Lee, and Jens Palsberg. Aurora: scalable sensor network simulation with precise timing. In *Proceedings of the 4th international symposium on Information processing in sensor networks, IPSN '05*, Piscataway, NJ, USA, 2005. IEEE Press.
 - [36] Yun Zhou, Yuguang Fang, and Yanchao Zhang. Securing wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials*, 10(1-4):6–28, 2008.

Appendix A

Content of attached CD

Content of the CD is following:

- source codes of implemented protocols along with simulation scenarios and tools;
- results in the ods format;
- thesis text in pdf format;
- thesis text in text format.