AN IMPROVED PACKET FORWARDING APPROACH FOR SOURCE LOCATION PRIVACY IN WIRELESS SENSORS NETWORK

MOHAMMAD ALI NASSIRI ABRISHAMCHI

A thesis submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2014

To my beloved family, who have much faith in me.

For their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to appreciate my supervisor **Professor Dr. Abdul Hanan Abdullah** for his support during my study at UTM. And also i would like to express heartfelt gratitude to my great mentors **Dr.Anazida Zainal and Dr.Abdur Razzaque** for their constant support during my study at UTM. They inspired me greatly to work in this project. They willingnesses to motivate me contributed tremendously to our project. I have learned a lot from them and I am fortunate to have them as my mentors and supervisors.

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities which I need during the process.

ABSTRACT

Privacy is one of the major concerns in dealing with information, either transmission or storage. The adversaries attempt to launch the variety of attacks against a system to capture their needed information. Sometimes content of information is their target and other times the context of information such as timing and location can be the aim of the attack. The wireless sensors network is established based on affairs related to information. Depending on the application of this type of networks, different security considerations should be taken. This research focuses on the source location privacy where the attacker tries to discover the origin sender of packets to achieve the under monitor assets by backtracking the received signals. The final aim is improving the safety period for source node and it means the prolonging the discovering duration of the exact location of source node for adversary. This study concentrates on solutions based on random walk method as a core technique and tries to present an idea to improve the results. The proposed approach named Isolated Adversary Zone is a solution for packet forwarding within wireless sensor network. In this study some of the existing methods are investigated in terms of safety period. These solutions have been implemented by simulating in MATLAB. From this knowledge, the author proposes a packet forwarding approach which can improve the safety period for source node. The proposed approach is tested and some future works are suggested at the end of this study.

ABSTRAK

Privasi merupakan salah satu perkara yang perlu dititikberatkan dalam menyimpan atau menghantar. Terdapat anasir-anasir jahat yang cuba untuk melancarkan pelbagai jenis serangan ke atas sistem bagi mendapatkan maklumat yang mereka perlukan tanpa kebenaran. Sasaran bagi serangan yang dilakukan merupakan isi kandungan di dalam maklumat tersebut dan selebihnya merupakan konteks yang berada di dalam maklumat seperti masa dan lokasi. Rangkaian pengesan tanpa wayar telah dibangunkan berdasarkan kepada perkara yang berkaitan dengan maklumat. Merujuk kepada penggunaan rangkaian pengesan ini, aspek keselamatan yang berbeza perlu diambil kira. Kajian ini bertumpu kepada privasi bagi sumber lokasi nod pengesan di mana penyerang cuba untuk mengesan penghantar asal paket bagi mencapai aset yang berada di bawah pengawasan dengan menjejak semula isyarat yang diterima. Matlamat akhir kajian ini adalah untuk meningkatkan tempoh keselamatan bagi nod sumber dan sekaligus memanjangkan lagi tempoh pencarian lokasi sebenar nod sumber oleh penyerang. Kajian ini memberikan fokus kepada penyelesaian berdasarkan kepada kaedah perjalanan rawak sebagai teknik utama dan cuba untuk memperbaiki kaedah tersebut. Pendekatan yang dicadangkan dinamakan sebagai Zon Pengasingan Penyerang yang merupakan penyelesaian untuk penghantaran paket di dalam rangkaian pengesan tanpa wayar. Dalam kajian ini, beberapa kaedah sedia ada telah dikaji dari segi tempoh keselamatan. Kaedah-kaedah ini telah diuji menggunakan simulasi dalam MATLAB. Berdasarkan kepada hasil pengujian ini, penulis telah membangunkan satu pendekatan penghantaran paket yang dapat meningkatkan tempoh keselamatan bagi nod sumber. Pendekatan yang dicadangkan ini telah diuji dan beberapa kerja penambahbaikan yang boleh dilakukan pada masa hadapan telah dicadangkan di akhir kajian ini.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

WSN	-	Wireless Sensors Network
QoS	-	Quality of Service
SLP	-	Source Location Privacy
AOA	-	Angle of Arrival
RSS	-	Received single Signal Strenght
PSPR	-	Phantom-Single Path Routing
DRW	-	Directed Random Walk
PDRW	-	Phantom-Directed Random Walk
IRL	-	Identity, Route and Location Privacy
R-IRL	-	Reliable Identity, Route and Location Privacy
STaR	-	Sink Toroidal Region Routing
PRESH	-	Probabilistic Reshaping
exPRESH	-	Extended Probabilistic Reshaping
RCAD	-	Rate Controlled Adaptive Delaying
DBT	-	Dynamic Bidirectional Tree
ZBT	-	Zig Zag Bidirectional Tree
CEM	-	The Cyclic Entrapment Method
iHIDE	-	Information Hiding in Distributing Environments
TTL	-	Time To Live

BUN	-	Bus Node
ACS	-	Anonymous Communications Scheme
APR	-	Anonymous Path Routing
CLS	-	Cross-layer Solution
DCLS	-	Double Cross-layer Solution
RP	-	Random Parallel
WRS	-	Weighted Random Stride Routing
ALbS	-	Anti Localization by Silencing
CALP	-	Context-Aware Location Privacy
LRTP	-	Lowering Radio Transmission Power
SLFSR	-	Flooding with Short Lived Fake Messages
PFSR	-	Flooding with Persistent Fake Messages
IAZ	-	Isolated Adversary Zone

CHAPTER 1

INTRODUCTION

1.0 Introduction

Wireless Sensor Network (WSN) is one of the well-known forms of networks which are consist of the numbers of sensor nodes with the capability of sensing events, brief processing on collecting raw data and transmitting processed data by hop-by-hop approach to the predefined destination with the aim of realizing controlling goals. These sensor nodes usually are designed application-specific.

There are numerous applications for this kind of networks, from health care to battlefield usages. Nowadays in every case that it is needed to collect data from environment based on the feasibility study and economic investigation one of the serious options might be WSN. This technology provides the ability of bringing under control the areas which they do not have the possibility of deploying wired network. For example, deploying wired networks in the depth of forests has huge cost or at the battlefields there is not possibility utterly. In the other hand, WSN can be applied to a battlefields by attaching tiny sensor node to the cloths of soldiers or spreading them in the certain area randomly and they perform duty of collecting vital data on the health status and also location of them and transmit data to headquarter.

In this case, it is clear the location of the source has a vital sensitivity, if an adversary is able to discover the location of event, then it can move there to capture the important items. In this situation the critical question is: how do we conceal the location of the nodes from the adversary? In fact, looking for the correct response to this question triggers researchers to provide privacy for the nodes, in the WSN research field it is recognized by “Location Privacy” which can be divided into source and sink location privacy.

In this thesis it has attempted to focus on “Source Location Privacy” as a specific subset of privacy within WSN. First the key concepts in source location privacy, such as safety period, and capture likelihood will be discussed. Then, we present an overview of existing solutions that provide source location privacy within a WSN in relation to the assumptions about the adversary’s capabilities. Proposing an improved routing solution and investigating the performance of it by simulating are the other goals of this thesis.

1.1 Problem Background

Due to a significant rise up of applications of digital circuits, obtaining noticeable progress in wireless transceivers and huge improvement in microprocessors, beside of new technologies in the field of batteries which can provide longer period energy rather than before in recent years, all the conditions become suitable for producing low cost sensor nodes in large size and does the applying of the WSN more particular and reasonable.

From the electronic architectural perspective, each sensor node consists of multiple components. Sensing unit which can consist of one or more sensor with the duty of gathering data from the environment. The processing unit which can have different level of power according to the application for performing initial process

on raw data. The communication unit has the responsibility to send and receive the information packets through the network. This unit consumes most of the available energy. The power unit is another component that provides the required energy for other units to perform their tasks. Figure 1.1 shows a schematic view of the architecture of sensor nodes (Zheng and Jamalipour 2009).

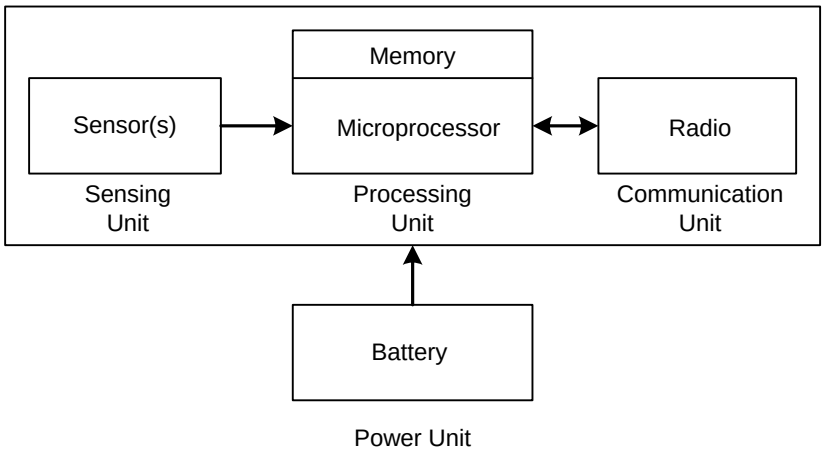

Figure 1.1 The Architecture of a Sensor Node in WSN

The eligible sensors which can participate in the WSN must have the capability of self-organizing, low cost and small size in the most of applications. Because of the high number of sensors which are spread randomly in the controlling zone, it is necessary that they be able to organizing their roles and positions automatically within the network and establish a reliable cooperation with their neighbors which are located in their transmitting range to launch the expected network. Also how much the cost of each sensor node decreases, it can be effective in different ways. For example, the saved money can spend on the increasing of the number of sensors to provide better monitoring ability or it can reduce the cost of whole network regarding to this fact that after finishing the life cycle of each sensor, in the majority of applications, it is gone and cannot reuse it again.

Wireless sensor nodes have some constraints such as limited storage, computing power, and energy supply which they force developers to find more effective

solutions which have low consumption in each of these parts as much as possible, because due to less consuming of resources of system, the life of nodes will increase. Among of all of these limitations, shortage of energy is more important rather than others. So, reducing the energy consumption by optimization of the active period of each unit is the common aim of the designers. Specifically, communication unit has the most energy consumption than others. Then, if the communication's goal come true with minimum possible sends and receives, it can affect the issue significantly.

However, the concerns about WSN will not be ended by hardware limitations. Regardless of all of them, still there are serious issues that must be considered. For example, if an adversary decides to compromise the network by performing various types of attacks, how much the threatened network is resistant? Answering to this question makes it clear that the existence of security considerations in designing policy of WSNs is a must. These networks usually carry important data related to specific areas which might be attractive for different types of adversaries, already there are a lot of different kinds of attacks which threat security and privacy of WSN, and they can put in danger all important requirements of a secure network such as confidentiality, integrity, availability and others. In the same way.

All related information about a WSN can be used by an adversary. So, all the aspects must be preserved as much as possible. For example, if an attacker by eavesdropping the data packets can be aware of the content of the message it can disclose critical information for an unauthorized party which such as incident can be very hurtful. For facing these kinds of threats, science of cryptography can be helpful. In other hand, sometime the contents of the messages are not interesting for enemies but they are looking for the location of the senders and receivers for different reasons. This willing will be achievable by tracking the packets regardless of their contents. Figure 1.2 illustrates a schematic view of this concept.

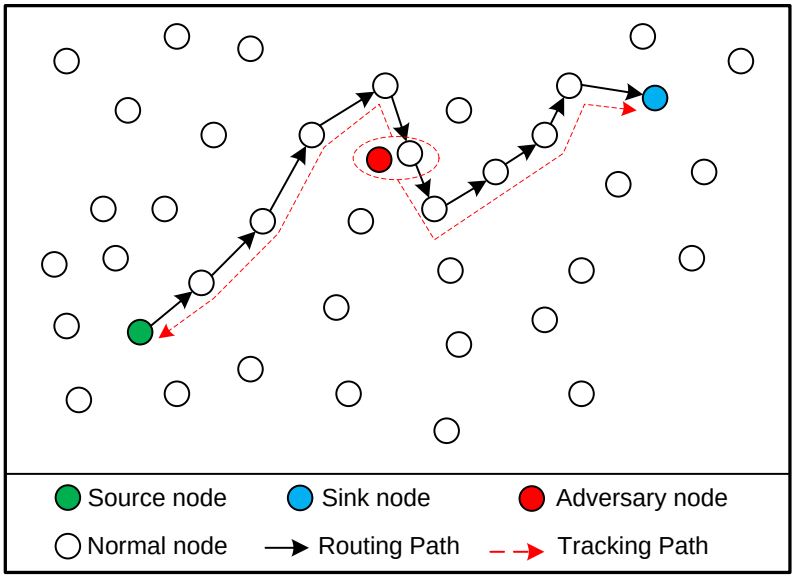

Figure 1.2 Discovering Scheme of the Location of Source Node

The nature of WSN, regardless of its benefits can be a potential weakness for it in security perspective. These networks has no fixed infrastructures and organized themselves based on their situation and also they use broadcast communication which has less security and an adversary can access to the transmission by benefit of various possibilities. In broadcast communication, it is not possible that you filter the receivers who are in the radio range but all the attempts are in the direction of making them meaningless for unauthorized receiver and create serious obstacles for the adversary to analysis the transmissions.

Wireless sensor networks suffer from many issues which limit the successful performance of it and due to various applications of this technology in high sensitivity areas, reliability in security and privacy is essential. In fact, the main issue of WSN is lack of general solution which can provide all requirements. For example, cryptography has a vast application in network communication and by using different method of encryption, it can prevent disclosure of information, but it is only useful in case of protecting the content of data packets. As explained above, context privacy is important as much as content privacy and in some specific

scenarios has a vital critical role, in some of these cases the content of packets are not interesting for the adversary but the location of communicators is most wanted.

Considering this example can be helpful for a clear understanding of this concept. Suppose a specific area with high security sensitivity are monitored by many security cameras which are deployed based on WSN principles and as a consequence of sensitivity, they must be hidden from the public to provide impalpable monitoring. Now, if an adversary is able to discover the cameras, monitoring project will fail. This malicious attack can be performed by techniques like back tracking or traffic analysis, depending on the strength of the adversary and the level of available devices. The adversary will stay close to the sink node to capture the packets and move to the location of immediate sender, until reaching to the location of origin node.

Performing the task of preserving transmissions of adversary requires generating of related routing protocols. As it is obvious, manipulating of basic routing protocols such that be able to provide reliable privacy need extra usage of resources and this issue will affect energy consumption in the last. The available energy in each node can determine the life duration of the node. So, providing appropriate tradeoff between satisfying security and privacy requirements and usage of resources is the most the challenging issues in this field of research. Also it is noticeable that this tradeoff should consider some other metrics such as quality of service (QoS) too.

All the solutions which claim enhance in the safety period, should be investigated in different prespectives, like energy consumption and deliver quality which consists of delivery latency and delivery ratio for identifying that they have real excellence or not. Figure 1.3 shows the relation between these three criteria (Conti, Willemsen et al. 2013).

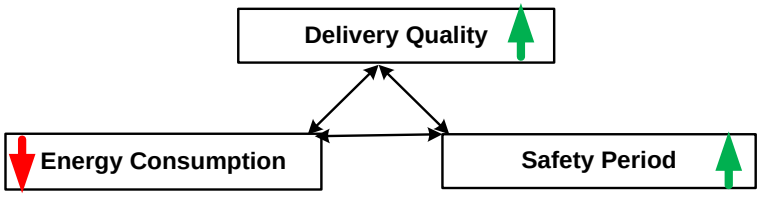

Figure 1.3 Relation Between Energy, Privacy and Performance

It is generally believed that the location privacy is an important vulnerability which is necessary to be overcome. For this purpose, many solutions are proposed by researchers. The suggested methods can be categorized in more than ten groups based on their core techniques, such as random walk, dummy packets, delay, geographic routing, cyclic entrapment, network location anonymization, cross layer routing, separate path routing, network coding, limiting detectability and others. Each of these core methods has a different solution under their category. It is considerable that the model of adversary is effective to select the solution to face it. For example, some of these methods are proposed to encounter with only local adversaries while some other pay attention to keep the source node location from global adversary. Also a few solutions are existing which target both general types of adversaries.

1.2 Problem Statement

The drawbacks which threat the location privacy of source nodes in wireless sensor network should be managed by increasing the safety period. This issue is one of the critical challenges in the field of security and privacy in WSN. The location of the source node should not be discoverable by the adversary while transmission, generally most common routing protocols cannot satisfy this demand with a cost effective manner in their packet forwarding approach.

Due to this weakness, it makes the practical application of WSN in the real world difficult especially in high sensitivity cases such as battlefields, healthcare and environment studies. Therefore, this study will address the following issues:

i. How to increase privacy level of source nodes in WSN.
ii. How to reduce the likelihood of discovery by an adversary.
iii. Which are the alternative approaches to prolong the safety period.

1.3 Purpose of Study

Regarding to the importance of hiding the location of source nodes in WSN which is very critical in some applications. This study attempts to increase the level of source privacy by proposing a new variant of solutions in this area which is called “Isolated Adversary Zone” in this project. This technique tries to conduct the adversary to the specific area far from the source and sink and keep it there to provide a safe path for transmitting rest of the messages. For measuring this factor in WSN, the amount of safety period is important and it means how long it takes to the location of source node be discovered by a local adversary who apply the backtracking technique as an attack.

This thesis also tries to provide some other results to show how this suggested way effects on the energy consumption of a routing protocol in WSN. Every variation in safety period will have a direct effect on other metrics, for this reason they must remain in reasonable level and every proposed design should pay attention to them.

1.4 Project Objectives

The objectives of this project are:

i. To measure the safety period of most important existing routing protocol based on the random walk approach. They are flooding, phantom-flooding and phantom-single path.
ii. To propose an improved design of a packet forwarding method that can prolong the safety period.
iii. To evaluate the proposed packet forwarding approach and compare it with investigated protocols in the first objective.

1.5 Project Scope

This research focuses on managing the stationary source location privacy within WSN (SLP in WSN) by proposing an improved forwarding solution based on below characteristic:

i. Random walks as a core technique. In this way, routing is based on picking neighbor nodes as an intermediary node in random fashion to confuse the adversary
ii. Local, patient, device rich third party as an adversary. Local adversary is posses physically inside the network and it is able to move from one node to another one, also it has same radio range with original nodes of the network. The adversary after moving to a new place beside of immediate sender, will wait there until capturing next packet. It is equipped with devices which can find the signal arrival angle, signal strength and strong processor.

iii. Backtracking as an attack technique, to discover the location of the source node. In this approach, the adversary starts from sink node and regarding to its captured signal, it moves hop by hop through the routing path to discover the origin node.

iv. Numbers of hops which adversary should backtrack as a metric of safety period. How much an adversary needs to cross more nodes in comparison with the shortest routing path, it means the improvement in safety period.

In below, Figure 1.4 shows the trend of narrowing the topic.

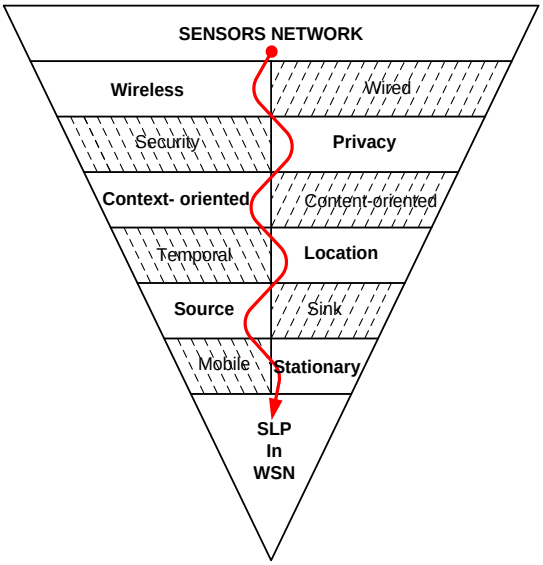

Figure 1.4 Focus of the Project

1.6 Significance of The Study

Wireless sensor network covers a vast research area. A lot of researchers are working on different aspects of it to develop the infrastructure and quality of

performance. One of the major areas in this filed is related to security and privacy, because regardless all of attempts to develop this technology, if an adversary be able to compromise it, applying this network will not be reasonable.

Undeniable useful application of the WSN and a lot of benefits of that technology makes it necessary to remove its vulnerabilities. One of the most important concerns is providing safety for all the aspects of network including hardware and software. If an unauthorized person is able to gain access to the network, he can interrupt performance of the network and it might lead to unrecoverable damages, then applying WSN will work in a negative direction. Specialists try to reduce the weaknesses all the time to make this technology more reliable. Source location privacy is one of their concerns. If an adversary can discover the position of sender node, he will have this capability to launch a variety of attacks against the system. For instance, an attacker can destroy the source node and stop monitoring of that special area also he can change the configuration by manipulating and extract more data from network to complete his knowledge about the system and based on them design a killer attack. Solving the problems in this field can increase the opportunities of applying it in the real world, especially in high sensitivity cases.

1.7 Thesis Structure

The thesis consists of 6 chapters. Chapter one describes the introduction, background of the study, research objectives and questions, the scope of the study and its primary objectives. The second chapter reviews available and related literature on source location privacy. Chapter three describes the study methodology along with the appropriate framework for the study. Chapter four provides the analysis the preliminary findings and design solutions for the proposed improvements. In chapter five, process of

implementation and achieved results are presented and eventually sixth chapter is dedicated to conclusion of this research.

REFERENCES

Alomair, B., et al. (2010). Statistical framework for source anonymity in sensor networks. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, IEEE.

Alomair, B., et al. (2013). "Towards a Statistical Framework for Source Anonymity in Sensor Networks."

Chen, H. and W. Lou (2010). From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks. Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International, IEEE.

Conti, M., et al. "Providing Source Location Privacy in Wireless Sensor Networks: A Survey."

Conti, M., et al. (2013). "Providing Source Location Privacy in Wireless Sensor Networks: A Survey."

Dutta, N., et al. (2010). Defending wireless sensor networks against adversarial localization. Mobile Data Management (MDM), 2010 Eleventh International Conference on, IEEE.

Fan, Y., et al. (2010). Preventing Traffic Explosion and Achieving Source Unobservability in Multi-Hop Wireless Networks Using Network Coding. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, IEEE.

Fan, Y., et al. (2009). An efficient privacy-preserving scheme against traffic analysis attacks in network coding. INFOCOM 2009, IEEE, IEEE.

Hong, X., et al. (2005). Effective probabilistic approach protecting sensor traffic. Military Communications Conference, 2005. MILCOM 2005. IEEE, IEEE.

Jhumka, A., et al. (2011). "On the use of fake sources for source location privacy: trade-offs between energy and privacy." The Computer Journal **54**(6): 860-874.

Jiang, J.-R., et al. (2011). "An Anonymous Path Routing (APR) Protocol for Wireless Sensor Networks." J. Inf. Sci. Eng. **27**(2): 657-680.

Kamat, P., et al. (2009). "Temporal privacy in wireless sensor networks: Theory and practice." ACM Transactions on Sensor Networks (TOSN) **5**(4): 28.

Kamat, P., et al. (2005). Enhancing source-location privacy in sensor network routing. Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, IEEE.

Kazatzopoulos, L., et al. (2006). ihide: Hiding sources of information in wsns. Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on, IEEE.

Li, N., et al. (2012). Using data mules to preserve source location privacy in wireless sensor networks. Distributed Computing and Networking, Springer**:** 309-324.

Li, N., et al. (2009). "Privacy preservation in wireless sensor networks: A state-of-the-art survey." Ad Hoc Networks **7**(8): 1501-1514.

Lightfoot, L., et al. (2010). Preserving source-location privacy in wireless sensor network using STaR routing. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, IEEE.

Majeed, A., et al. (2009). TARP: Timing Analysis Resilient Protocol for Wireless Sensor Networks. Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on, IEEE.

Mehta, K., et al. (2007). Location privacy in sensor networks against a global eavesdropper. Network Protocols, 2007. ICNP 2007. IEEE International Conference on, IEEE.

Osborne, M. J. and A. Rubinstein (1994). A course in game theory, MIT press.

Ozturk, C., et al. (2004). Source-location privacy in energy-constrained sensor network routing. Workshop on Security of ad hoc and Sensor Networks: Proceedings of the 2 nd ACM workshop on Security of ad hoc and sensor networks.

Ozturk, C., et al. (2004). Source-location privacy in energy-constrained sensor network routing. SASN.

Rios, R. and J. Lopez (2011). "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks." The Computer Journal **54**(10): 1603-1615.

Roy, S., et al. (2010). A survey of game theory as applied to network security. System Sciences (HICSS), 2010 43rd Hawaii International Conference on, IEEE.

Shaikh, R. A., et al. (2010). "Achieving network level privacy in wireless sensor networks." Sensors **10**(3): 1447-1472.

Shao, M., et al. (2009). Cross-layer enhanced source location privacy in sensor networks. Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, IEEE.

Sheu, J.-P., et al. (2008). Anonymous path routing in wireless sensor networks. Communications, 2008. ICC'08. IEEE International Conference on, IEEE.

Spachos, P., et al. (2010). Opportunistic routing for enhanced source-location privacy in wireless sensor networks. Communications (QBSC), 2010 25th Biennial Symposium on, IEEE.

Suarez-Tangil, G., et al. (2010). An experimental comparison of source location privacy methods for power optimization in WSNs. Proceedings of the 3rd WSEAS international conference on Advances in sensors, signals and materials, World Scientific and Engineering Academy and Society (WSEAS).

Tavli, B., et al. (2010). "Mitigation of compromising privacy by transmission range control in wireless sensor networks." Communications Letters, IEEE **14**(12): 1104-1106.

Wang, H., et al. (2009). "Privacy-aware routing in sensor networks." Computer Networks **53**(9): 1512-1529.

Xiao, M., et al. (2010). "Privacy Preserving Hop-distance Computation in Wireless Sensor Networks." Chinese Journal of Electronics **19**(1): 191-194.

Yang, Y., et al. (2008). Towards event source unobservability with minimum network traffic in sensor networks. Proceedings of the first ACM conference on Wireless network security, ACM.

Yao, J. and G. Wen (2008). Preserving source-location privacy in energy-constrained wireless sensor networks. Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on, IEEE.

Yick, J., et al. (2008). "Wireless sensor network survey." Computer Networks **52**(12): 2292-2330.

Zheng, J. and A. Jamalipour (2009). Wireless sensor networks: a networking perspective, Wiley. com.