UNIVERSITI PUTRA MALAYSIA

DANGER THEORY BASED NODE REPLICATION ATTACK DETECTION AND MITIGATION IN CLUSTER MOBILE WIRELESS SENSOR NODES

HAAFIZAH RAMEEZA SHAUKAT

DANGER THEORY BASED NODE REPLICATION ATTACK DETECTION AND MITIGATION IN CLUSTER MOBILE WIRELESS SENSOR NODES

By

HAAFIZAH RAMEEZA SHAUKAT

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

September 2014

COPYRIGHT

DEDICATIONS

In the name of Allah, Most Gracious, Most Merciful

This thesis is dedicated to:

My caring and devoted parents for their unconditional love and support

And

My dearest fiance, sister, brothers and friends, for their whole-hearted and substantial support

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

DANGER THEORY BASED NODE REPLICATION ATTACK DETECTION AND MITIGATION IN CLUSTER MOBILE WIRELESS SENSOR NODES

By

HAAFIZAH RAMEEZA SHAUKAT

September 2014

Chairman: Fazirulhisyam Hashim, PhD

Faculty: Engineering

Mobile wireless sensor networks (MWSNs) comprise a collection of mobile sensor nodes with confined and finite resources. They commonly operate in hostile environments such as battle fields and surveillance zones, and due to their operating nature, MWSNs are often unattended, and generally are not equipped with tamper-resistant tools. With little effort, an adversary may capture the nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Therefore, the detection of node replication attacks in MWSN is very important. Existing node replication detection schemes depend primarily on centralized mechanisms with single points of failure and slow detection. Moreover, majority of the schemes do not consider node mobility, thus are unsuitable for implementation in MWSN environment. To address these fundamental limitations, this thesis utilizes the concept of Danger Theory (DT) to secure MWSN from node replication attacks. The DT operates based on a multilevel detection, thereby improving the detection of replica in the network. According to this theory, whenever the meeting frequency of any two nodes in the MWSN goes beyond a certain threshold (i.e., derived based on nodes location and time interval), the witness node will broadcast security message to base station (BS), which is then responsible to set up a Danger Zone (DZ) around the infected cluster. Sensor nodes within the DZ area will then initiate the next level of detection and mitigation process by exchanging security information among them. Specifically, the proposed DT scheme is categorized into three stages, namely the 1st level detection, 2nd level detection and 3rd level detection. To recognize malicious replica in MWSN, the first approach is used to highlight the possibility of replica attack and to identify the infected area in the MWSN. The second approach is used to mitigate the attacks by focusing on the fact that a

replica node always has higher voltage compared to the original one, as replica is generated after the deployment of the original node or password check. Lastly, the third approach is used to protect the network (i.e., mitigation process), as BS will alert other BSs (and nodes) about the existence of replica. The evaluations of the proposed scheme in respect of security features and performance overheads are carried out through intensive analysis and simulations, as well as extensive comparison with other schemes. The findings from these evaluations indicate that the proposed DT based node replica detection achieve robust, fast and effective detection (i.e., true positive more than 90%, false positive less than 1% and false negative less than 0.2% rates) while introducing reasonable overheads.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

PENGESANAN DAN PENGURANGAN SERANGAN REPLIKASI NOD BERASASKAN TEORI BAHAYA DALAM KLUSTER NOD BERGERAK SENSOR TANPA WAYAR

Oleh

HAAFIZAH RAMEEZA SHAUKAT

September 2014

Pengerusi: Fazirulhisyam Hashim, PhD

Fakulti: Kejuruteraan

Rangkaian bergerak sensor tanpa wayar (MWSNs) terdiri daripada koleksi nod sensor mudah alih dengan sumber terhad dan terbatas. Mereka biasanya beroperasi dalam persekitaran seperti medan perang dan zon pengawasan, dan berdasarkan sifat operasi mereka, MWSNs secara amnya tidak dilengkapi dengan alat tahan gangguan. Musuh boleh mencuri nod, menganalisis dan meniru nod, dan secara tersembunyi memasukkan replika ini di lokasi-lokasi strategik di dalam rangkaian. Serangan seperti itu boleh membawa kesan yang teruk. Musuh dengan mudah boleh merosakkan sistem rangkaian atau menghentikan operasi bahagian-bahagian penting di dalam rangkaian. Oleh itu, pengesanan serangan replikasi nod dalam MWSN adalah penting. Skim pengesanan replikasi nod yang sedia ada bergantung terutamanya pada mekanisme berpusat dengan titik tunggal kegagalan dan pengesanan yang lambat. Selain itu, majoriti skim tidak mengambil kira mobiliti nod, oleh itu ia tidak sesuai untuk dilaksanakan dalam persekitaran MWSN. Untuk menangani batasan asas ini, tesis ini menggunakan konsep Teori Bahaya (DT) untuk menjamin MWSN selamat daripada serangan replikasi nod. DT beroperasi berdasarkan pengesanan pelbagai peringkat, dengan itu meningkatkan pengesanan replika dalam rangkaian. Menurut teori ini, setiap kali perjumpaan kekerapan dari mana-mana dua nod dalam MWSN melampaui aras tertentu (iaitu , yang diperolehi berdasarkan lokasi dan masa selang nod itu), nod saksi akan menyiarkan mesej keselamatan ke stesen pangkalan (BS), yang kemudiannya bertanggungjawab untuk menubuhkan sebuah Zon Bahaya (DZ) di sekitar kelompok yang dijangkiti. Nod sensor di dalam kawasan DZ seterusnya akan ke peringkat pengesanan dan proses pengurangan dengan bertukar-tukar maklumat keselamatan di kalangan mereka. Khususnya, skim DT yang dicadangkan dikategorikan kepada tiga peringkat, iaitu pengesanan tahap 1, pengesanan tahap 2 dan pengesanan tahap 3. Untuk mengiktiraf replika berniat jahat dalam MWSN, pendekatan yang pertama digunakan untuk menyerlahkan kemungkinan serangan replika dan untuk mengenal pasti kawasan yang dijangkiti dalam

MWSN itu. Pendekatan kedua digunakan untuk mengurangkan serangan dengan memberi tumpuan kepada hakikat bahawa nod replika sentiasa mempunyai voltan yang lebih tinggi berbanding dengan yang asal, di mana replika dihasilkan selepas penempatan nod asal atau cek kata laluan. Selain itu, pendekatan yang ketiga digunakan untuk melindungi rangkaian, yang mana BS akan memberi isyarat kepada BSS lain (dan nod) tentang kewujudan replika di MWSN itu. Penilaian skim yang dicadangkan bagi ciri-ciri keselamatan dan overhed prestasi dijalankan melalui analisis dan simulasi intensif, dan juga perbandingan secara meluas dengan skim lain. Penemuan daripada penilaian ini menunjukkan bahawa nod DT berdasarkan replika pengesanan yang dicadangkan mencapai tahap pengesanan yang teguh, cepat dan berkesan (iaitu, kadar positif benar lebih daripada 90%, positif palsu kurang daripada 1% dan negatif palsu kadar kurang daripada 0.2%) dengan overhed yang berpatutan.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Dr. Fazirulhisyam Hashim for his generous support and great encouragement to conduct this research as well as his valuable comments to enhance the dissertation's quality.

Also, I am very grateful to Assoc. Prof. Dr. Aduwati Binti Sali and Assoc. Prof. Dr. Fadlee Bin A Rasid as the other member of my supervisory committee for their invaluable help and support to achieve my research goals and objectives. Furthermore, I would like to appreciate department staff and my research group fellows for their great cooperation and assistance during my research and thesis writing.

APPROVAL SHEET 1: Examination Committee

I certify that a Thesis Examination Committee has met on **24th October 2014** to conduct the final examination of **Haafizah Rameeza Shaukat** on her thesis entitled "**DANGER THEORY BASED NODE REPLICATION ATTACK DETECTION AND MITIGATION IN CLUSTER MOBILE WIRELESS SENSOR NODES**" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the **Degree of MASTER of Science**.

Members of the Thesis Examination Committee were as follows:

Dr. Abdul Rahman b. Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairperson)

Dr. Shaiful Jahari b. Hashim, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Dr. Shamala K. Subramaniam, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Dr. Sabira Khatun, PhD
Professor
School of Computer and Communication Engineering
Universiti Malaysia Perlis (UniMAP)
(External Examiner)

...., PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.

The members of the Supervisory Committee were as follows:

Fazirulhisyam b. Hashim, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairperson)

Aduwati Sali, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Mohd Fadlee b.A. Rasid, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG B.K. HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: _____

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____	Signature: _____
Name of Chairman of Supervisory Committee: _____	Name of Member of Supervisory Committee: _____
Signature: _____	Signature: _____
Name of Member of Supervisory Committee: _____	Name of Member of Supervisory Committee: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BS	Base Station
CDD	Cooperative Distributed Detection
CA	Collision Avoidance
CH	Cluster Head
CO	Communication Overhead
CS	Co-stimulation Signal
CSMA	Carrier Sense Multiple Access
DoS	Denial of Service
DT	Danger Theory
DZ	Danger Zone
EDD	Efficient Distributed Detection
FP	False Positive
FN	False Negative
ID	Identity
IP	Initiation Process
IS	Initiation Signal
LCA	Location Claim Approach
LSM	Line Selected Multicast
MAC	Medium Access Control
MANET	Mobile Adhoc Network
MC	Memory Cost
MCW	Mobile Centralized and Whole
MDW	Mobile Distributed and Whole
MGA	Multi Group Approach
MTLSD	Multi Time Location Storage and Diffusion
MWSN	Mobile Wireless Sensor Network
n	Number of nodes
NDFD	Non-deterministic and fully distributed
P-MPC	Parallel Multiple Probabilistic Cells
R	Right
RED	Randomized Efficient and Distributed
RM	Randomized Multicast
RP	Recognition Process
RS	Recognition Signal
RWPM	Random Way Point Mobility
SCRW	Static Centralized Random uniform and Whole
SDC	Single Deterministic Cell
SDD	Simple Distributed Detection
SDGW	Static Distributed Grid and Whole
SDGL	Static Distributed Grid and Local
SDRW	Static Distributed Random uniform and Whole
SEDD	Storage Efficient Distributed Detection
SHD	Single Hop Detection

SPRT	Sequential Probability Ratio Test
TDMA	Time Division Multiple Access
TP	True Positive
UTLSE	Unary Time Location Storage and Exchange
VP	Verification Process
W	Wrong
WSN	Wireless Sensor Network
XED	eXtremely Efficient Detection

CHAPTER 1

INTRODUCTION

1.1 Background

Mobile wireless sensor networks (MWSN) are used to effectively address countless challenging issues of monitoring and performing different tasks in our daily routine. MWSN is generally being practiced in applications like military operations, intelligence activities, monitoring communication, controlling devices, and surveillance activities in different environment. The advantage of using mobile node is that it has the ability to move and sense by itself. Due to the multi operations of MWSN in many applications, the current research focuses on effectiveness of energy, communication overhead and protocols in MWSN [1].

Recently, MWSN has become important for dealing with security threats and monitoring issues [2]. In many applications, the security issues are related to energy computation, monitoring and communication performance evaluation of the network [3]. To eliminate the security threats, networks should be modified with respect to methods like monitoring, communication approaches and surveillance. Nodes deployment is necessary for performance analysis, effectiveness and evaluation of different parameters in MWSN. Recent research has shown that features of mobility reduce many problems instead of making them complex. Therefore, the mobile nodes are important and necessary modules in wide range applications of sensor networks.

A mobile node consists of battery, micro-controller, communication device, memory, sensors and mobility features. The sensor node's functionality, effectiveness and value can be improved by using mobility. Mobile nodes can be used to reduce installation costs, extend the connectivity to wireless, enhance the latitude in various applications, establish a robust behavior in varying environmental conditions and sustain complete coverage in limited period [2]. Mobile node operates with comprehensive analysis on channel connectivity models, mobility, obstacles design, communication protocols and graphical representation of wireless developments [4]. An analytical analysis on connectivity issues and understating of various performances has been provided through MWSN model. The performance metrics in MWSN are coverage, uniformity, time and distance [5].

MWSN has extra valuable functionality compared to WSN in term of coverage, data routing, data mulling, user access point and intermediate data. The mobile node has brought distinct challenges in terms of coverage, resource management, routing protocols and security. The mobility feature has advantages as well as some problems in sensor networks such as time and space consideration. While gathering information and data, processing can be delayed due to moving nodes and positioning effect of nodes. The mobile nodes are responsible for establishing

connection, gathering, transferring and delivering information. Moreover, the mobile node has the ability to randomly move, transfer and swap locations[6]. In MWSNs, mobile nodes perform important tasks, provide efficient operations in different applications and can sort out many security issues and have more benefits than static WSNs.

In MWSN, there are several kinds of security threats like jamming, wormhole, node replication, black hole, SYBIL, denial of service (DoS), privacy based, hello flood, physical attacks, routing attacks and so on. Subsequently, MWSN is typically an unattended nature network and consists of low cost sensors nodes. In MWSN, node replication threat is a dangerous problem. An attacker compromises a mobile node so that he can gain the whole data saved in the node and can produce multiple replica. A replication attack is essentially based on how fast an attacker is able to collect the data for malicious activities.

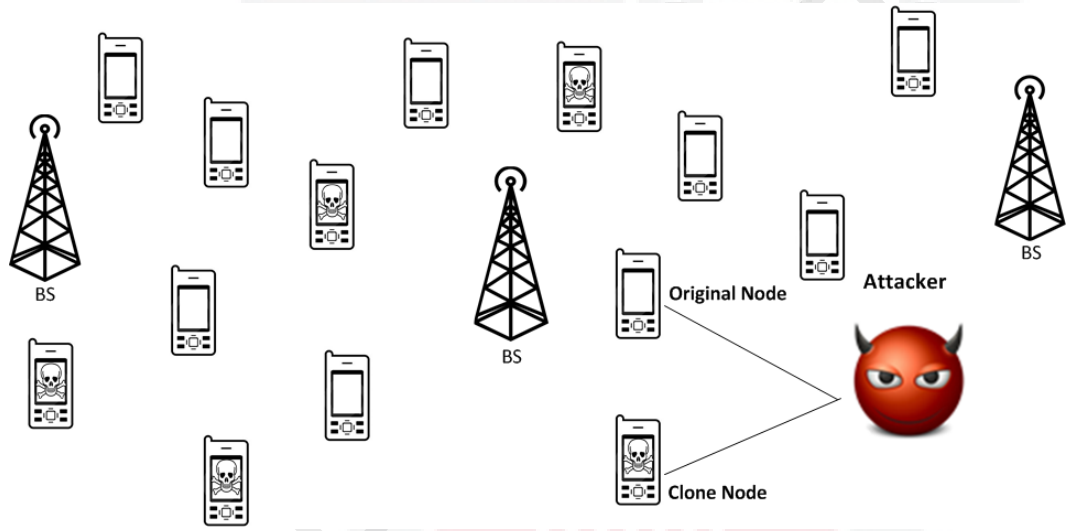

Figure 1.1: Node replication attacks.

Figure 1.1 shows the scenario of replication attack generated by the attacker. It illustrates how node replication attacks are initiated by an attacker in MWSN. An attacker utilizes the benefits of unattended behavior to capture the mobile node and retrieve the information from the nodes memory, for example, its identity, key, communication data and so on. Additionally, attacker can replicate the compromised node and send it back into the target area. After a mobile node is captured, an attacker can generate multiple replicas of the node to monitor and control the whole network. It is very dangerous for the network as it can restrict it, if it is not detected quickly.

Currently, the main focus of the research is to capture and resolve the issue regarding the replication attacks with mobility features in an effective and timely manner. In this thesis, experience is utilized to explain the procedure for analyz-

ing the design of various parameters of MWSN and to provide an approach to get better performance, evaluation and outcomes [7]. In this thesis, the main focus is to elaborate the concept of Danger Theory (DT) for node replica detection in MWSNs. This research initiates the idea of DT approach for replica detection based upon multilevel of detection in MWSNs. The introduction of DT based detection solution approach in the research field is drawn from motivations and incentive for secure mechanisms with the intention to support the detection and mitigation of attacks and to provide a suitable and secure solution (i.e., to detect replica at different level). The proposed multilevel detection framework contains three levels of detection; 1st level detection (i.e., cluster based), 2nd level detection (i.e., voltage comparison or password checking) and 3rd level detection (i.e., network protection).

For governing the presence of clones, the DT based detection approach adopts the theory of multiple level detection schemes. At present, there is no known research based on multilevel detection for replication attacks detection in MWSN. The literature review justifies the prospect of implementing the DT into node replication attacks in MWSNs. Since the existing solutions for replica detection in MWSNs have been illustrated to have some disadvantages, it is necessary to introduce new concept such as the DT approach (i.e., multilevel detection) for replication attacks detection. Furthermore, the DT approach employs the idea of the multilevel detection in the network to detect a replica. This approach is used to highlights the Danger Zone (i.e., DZ), which reflects the concept of focusing only on the danger area (i.e., DZ) to prevent the network from malicious activities instead of involving whole network.

1.2 Problem Statement and Motivation

Tamper resistant hardware is expensive, so most wireless sensor networks (WSN) are composed of unshielded sensor nodes. An attacker can capture, evaluate and reprogram the unshielded mobile nodes and then compose multiple replicas and send them into the network for malicious activities. It is very hard and complex to distinguish the clone node from the real node. For MWSN it is considered that the attacker is also mobile. Therefore, the detection of node replication attacks in MWSN is a crucial issue. Existing node replication detection schemes depend primarily on centralized mechanisms with single points of failure and slow detection. It will concisely deliberate how to centralize and distribute schemes for replica detection effectively in MWSN. The centralized schemes may affect the network performance due to single point of failure [8]. In addition, the mobile nodes nearest to the central point may have increased load and create congestion. This would be beneficial to the attacker. Accordingly, SPRT [9, 10] is fast clone detection strategy based on the comparison of speed with certain threshold, so it needs accurate measurements devices which are too expensive and may not be affordable. Furthermore, if the attacker is very intelligent he or she can set the node at different speed.

To resolve the single point of failure issue, a distributed approach has been proposed. By observing different distributed strategies, it has been noted that each method depends on the time of node's meeting. XED [11] is based on exchanging the random number, and is not a fast detection as it depends on the time these nodes meet with each other and exchange the numbers. Moreover, majority of the schemes do not consider node mobility, thus are unsuitable for implementation in MWSN environment. Therefore, a quick and fast detection is required to treat and resolve this security issue. Otherwise it will create a great danger for the whole network communication. For network protection, a quick and efficient detection is important to eliminate the harmful, dangerous and monitoring activities. In order to reduce the above issues, the DT hybrid (i.e., centralized and distributed) based approach is used for replica detection in MWSN.

1.3 Research Challenges and Issues

Nowadays, mobile sensor nodes are commonly used in different activities (such as military, weather, medical and agriculture and others) and have a great security concern. As in MWSN, the detection of node replication attack is distant changed, but more complex and challenging than in WSN.

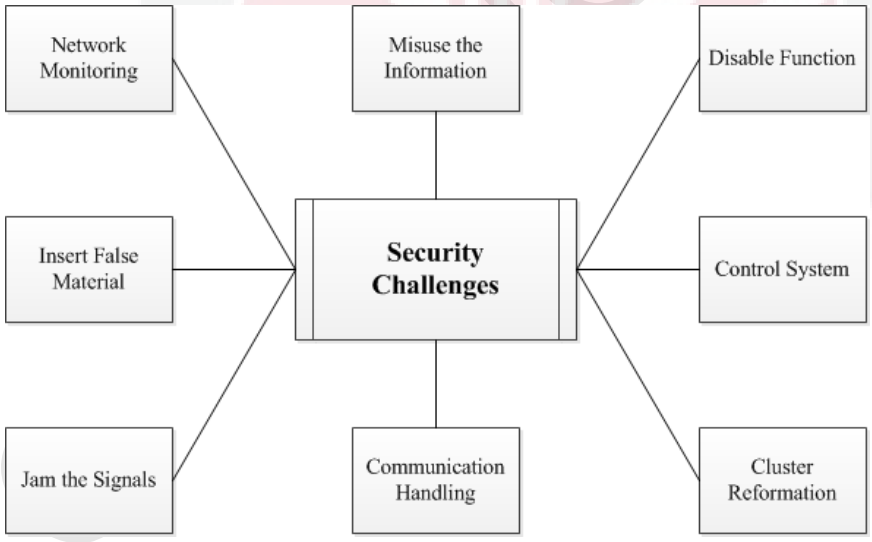

Figure 1.2: Security challenges of node replicas in WSN.

Conventionally, it is a great concern to resolve the threat in sensor network from advisory. The attacker can easily do the following tasks in minimum time duration:

1. Monitor the whole network communication
2. Control the WSN

3. Insert false information
4. Jam the signals
5. Change the formation of cluster
6. Handle the different protocols
7. Disable the function of Network
8. Misuse of the mobile nodes for malicious activities

Figure 1.2 illustrates the challenges regarding detection of replicas in MWSN. There is a probability that if the mobile replica is not detected quickly and accurately, it would be very harmful to the network. This is because in a minimum time period, the attacker can capture the whole network information. Therefore, a quick, accurate and efficient detection is required to eliminate the replicas from network.

1.4 Aims and Objectives

The motivation behind this research is to resolve the security issues regarding clone attacks in MWSN. In light of these security issues, the proposed method should also have emphasis on clone mitigation process instead of clone detection only. The multilevel detection (i.e., hybrid) approach based on danger theory namely, 1st level detection, 2nd level detection and 3rd level detection are considered in this study. The DT based detection framework will be evaluated based on various performance features such as detection accuracy, network lifetime, energy consumption, detection rate, communication overhead and memory cost, to showing the effectiveness of proposed research in MWSN. The danger theory approach (i.e., multilevel detection) will not only simplify the clone detection process step by step, but also capable to highlighting the specific area (i.e., danger zone) for the detection and mitigation of clone attacks. The main aim of this research is to protect MWSN from node replication attacks. In order to achieve aforementioned aim, the following objectives need to be accomplished:

1. To design, implement and evaluate an efficient node replication detection in MWSN based on multilevel detection (i.e., danger theory hybrid based) security framework. The proposed DT approach should achieve the following tasks for an efficient clone detection:

    - To design the security performance evaluation (i.e., detection accuracy) in terms of high true positive rate and low false positive and false negative rates.
    - To simulate a feasible model with minimizing the communication and memory overhead.

- To evaluate a fast clone detection and mitigation process in an effective manner to secure the network from malicious activities.

2. To further secure MWSN from node replication attacks by incorporates mitigation process (i.e., update information to the other networks about presence of clone) in the proposed DT (i.e., multilevel detection) method.

1.5 Thesis Scope

An intention for the detection of replication attacks have improved for next generation networks with security aspects in MWSN. With an attention, that the detection method should not emphasize only on replica detection but also on network protection from dangerous security attacks. In MWSN, the protection from security attacks like node replication attack is extremely challenging. The security concerns due to node replication attacks as discussed in the primary section highlight the motivation for establishing security framework to secure the MWSN.

Another goal of this research is to emphasize not only on clone detection but also on network protection (i.e., mitigation process) from dangerous security attacks. The proposed method described how the clone node can be accurately detected by mentioning the particular area (i.e., Danger Zone) instead of the whole network. This thesis proposes detection method based on the DT (Danger Theory) hybrid (centralized and distributed) based approach (i.e., multilevel detection) for protection from replication attacks at networks (MWSN) level. The multilevel detection mechanism applicability is considered by using security metrics of true positive, false positive and false negative rate. The proposed approach also demonstrates that the DT (Multilevel detection) method is competent and effective in terms of replica detection, mitigation from malicious activities and updating other networks about replicated node, thus enhancing and improving the MWSNs survivability.

1.6 Limitations of the Study

The proposed method assumes both original and clone nodes are present in the network with the same identity (i.e., two or multiple clone nodes) and the batteries are not rechargeable, for example by the use of solar cells. It will be complex to control the situation when rechargeable batteries are used because in this way original nodes can be mistakenly declared as replica ones. It is assuming that the same battery type is being used at a time because the value of the node voltage depends upon its type. It also considers that each node has its own private key. Moreover, the proposed method is not valid for single replica (i.e., there is a possibility that attacker restores only the replicated node in the network instead of both original and replica).

1.7 Study Module

The summary of the proposed DT approach for replication attacks detection is illustrated in Figure 1.3, where the solid lines with colored boxes indicate the followed track to achieve the determined objectives and the dashed lines with white box illustrate the research fields within WSN which have not been discussed in this research.

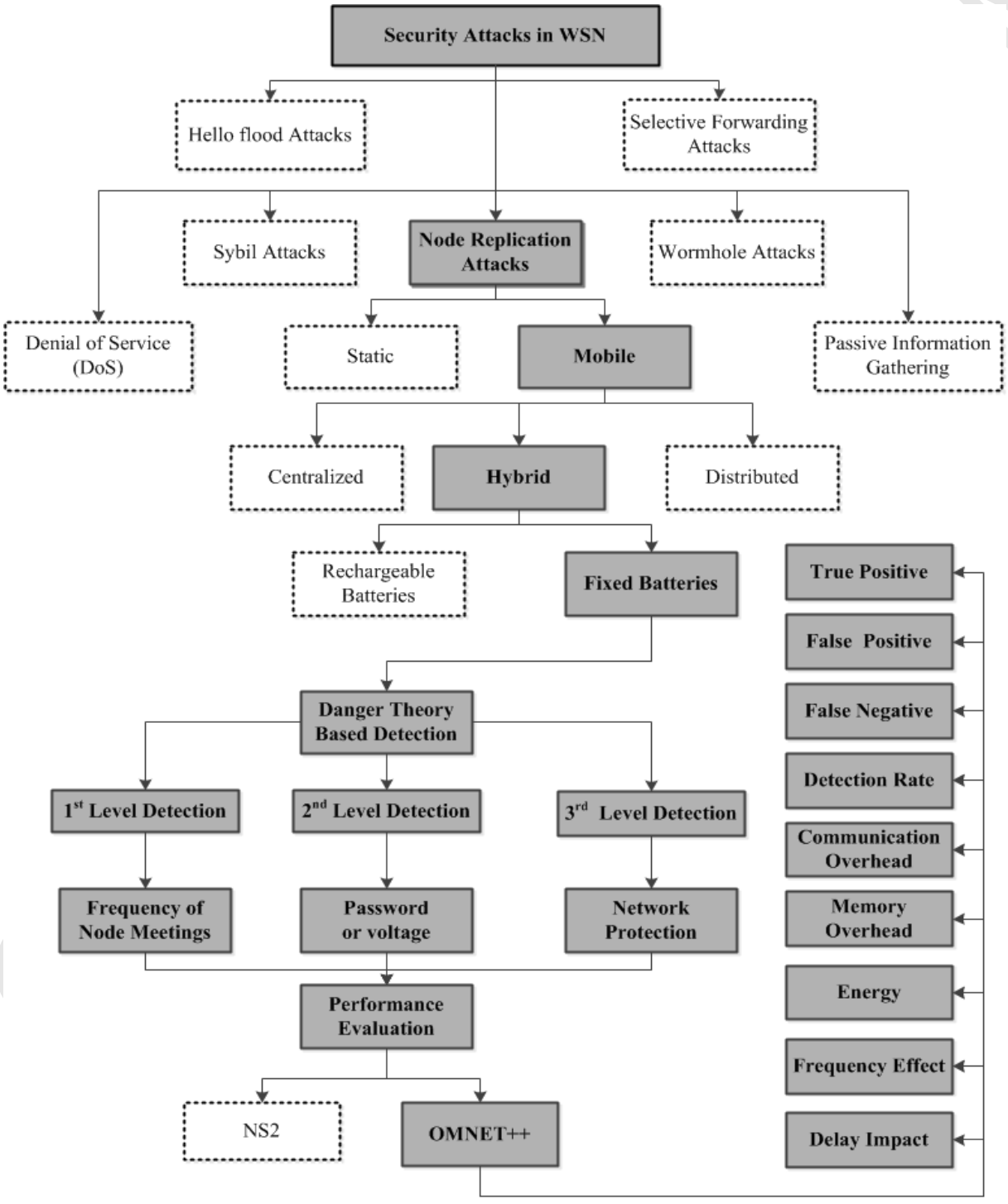

Figure 1.3: Study module.

1.8 Thesis Organization

This thesis is organized as follows:

Chapter 1 presents a brief introduction to the node replication attacks in MWSN. It explains, how node replica is generated in MWSN and the challenges faced to secure the network from these attacks. This chapter also includes the problem statement, research challenges and issues, objectives, thesis scope and limitation of the study.

Chapter 2 provides the detail of traditional security measures and security goals in WSN and MWSN. The comparison between MWSN and static WSN is also discussed. It also highlights the effect of security goals on node replication attacks. The main focus of this chapter is to explain the overview of all previous works done on mitigation and detection of clones attacks in MWSN. The subsequent sections also explain the comparison of existing approaches. Furthermore, this chapter also explains the research issues and open trends in detail, which lead to the concept of the Danger Theory (DT).

In chapter 3, the proposed methodology for detecting node replication attacks is explained thoroughly by considering the three main levels of detection in MWSN, namely, 1st level detection, 2nd level detection and 3rd level detection. Subsequently, the DT approach (hybrid based) architecture and simulation parameters are explained. A competent clone node detection (i.e., hybrid approach) approach is pointed out by performance evaluation, simulation scenarios, mathematical formulas and security parameters, using danger theory multilevel detection based solution in MWSN. Basically it depends on multiple level of detection (i.e., 1st level of detection, 2nd level of detection and 3rd level detection). 1st level of detection is based on the frequency of node meeting, if it exceeds a certain threshold, it would be an indication of attack. 2nd level of detection is initiated after indication of attacks in MWSN and it is a second security check based on password check or voltage comparison. 3rd level of detection is introduced to inform about replica to all base station.

Chapter 4 illustrates the simulation results of the proposed secure, efficient, competent solution approach and algorithm by using output graphs, tables and diagrams. The performance evaluation and simulation results show that the proposed method is more authentic, quick, efficient, competent and powerful in detecting replica.

Finally in Chapter 5, the thesis concludes with a summary of research achievements, some concluding remarks and recommended future work.

REFERENCES

[1] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[2] Noureddine Boudriga and Mohammad S Obaidat. Mobility and security issues in wireless ad-hoc sensor networks. In *IEEE Global Telecommunications Conference, 2005. GLOBECOM'05.*, volume 5, pages 5–pp. IEEE, 2005.

[3] Li Zhou, Jinfeng Ni, and Chinya V Ravishankar. Supporting secure communication and data collection in mobile sensor networks. In *INFOCOM*, 2006.

[4] Saad Ahmed Munir, Biao Ren, Weiwei Jiao, Bin Wang, Dongliang Xie, and Man Ma. Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing. In *21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW'07*, volume 2, pages 113–120. IEEE, 2007.

[5] Jin Zhu, Symeon Papavassiliou, and Sheng Xu. Modeling and analyzing the dynamics of mobile wireless sensor networking infrastructures. In *Proceedings 2002 IEEE 56th Vehicular Technology Conference, VTC 2002-Fall*, volume 3, pages 1550–1554. IEEE, 2002.

[6] Xuhui Chen and Peiqiang Yu. Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes. In *2010 3rd International Conference on Biomedical Engineering and Informatics (BMEI)*, volume 7, pages 2863–2867. IEEE, 2010.

[7] Ugo Maria Colesanti, Carlo Crociani, and Andrea Vitaletti. On the accuracy of omnet++ in the wireless sensornetworks domain: simulation vs. testbed. In *Proceedings of the 4th ACM workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pages 25–31. ACM, 2007.

[8] Bo Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia, and Sankardas Roy. Efficient distributed detection of node replication attacks in sensor networks. In *ACSAC 2007 Twenty-Third Annual Computer Security Applications Conference, 2007*, pages 257–267. IEEE, 2007.

[9] Jun-Won Ho, Matthew Wright, and Samir K Das. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. In *IEEE INFOCOM 2009*, pages 1773–1781. IEEE, 2009.

[10] Jun-Won Ho, Matthew Wright, and Sajal K Das. Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing. *IEEE Transactions on Mobile Computing*, 10(6):767–782, 2011.

[11] Chia-Mu Yu, Chun-Shien Lu, and Sy-Yen Kuo. Mobile sensor network resilient against node replication attacks. In *5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08*, pages 597–599. IEEE, 2008.

[12] Roberto Di Pietro, Luigi V Mancini, Claudio Soriente, Angelo Spognardi, and Gene Tsudik. Data security in unattended wireless sensor networks. *IEEE Transactions on, Computers*, 58(11):1500–1511, 2009.

[13] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

[14] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *Proceedings in Symposium on Security and Privacy, 2003*, pages 197–213. IEEE, 2003.

[15] Wen Tao Zhu, Jianying Zhou, Robert H Deng, and Feng Bao. Detecting node replication attacks in wireless sensor networks: A survey. *Journal of Network and Computer Applications*, 35(3):1022–1034, 2012.

[16] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2):293–315, 2003.

[17] Mark Luk, Ghita Mezzour, Adrian Perrig, and Virgil Gligor. Minisec: a secure sensor network communication architecture. In *IPSN 2007, 6th International Symposium on Information Processing in Sensor Networks, 2007*, pages 479–488. IEEE, 2007.

[18] Radha Poovendran, Cliff Wang, and Sumit Roy. *Secure Localization and Time Synchronization: For Wireless Sensor and AD Hoc Networks*, volume 30. Springer, 2006.

[19] Bo Sun, Lawrence Osborne, Yang Xiao, and Sghaier Guizani. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Wireless Communications*, 14(5):56–63, 2007.

[20] Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, and TT Abdelzaher. Pda: Privacy-preserving data aggregation in wireless sensor networks. In *INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, pages 2045–2053. IEEE, 2007.

[21] Bryan Parno, Adrian Perrig, and Virgil Gligor. Distributed detection of node replication attacks in sensor networks. In *2005 IEEE Symposium on Security and Privacy*, pages 49–63. IEEE, 2005.

[22] Yingshu Li, My T Thai, and Weili Wu. *Wireless sensor networks and applications*. Springer, 2008.

[23] Fei Hu and Neeraj K Sharma. Security considerations in ad hoc sensor networks. *Ad Hoc Networks*, 3(1):69–89, 2005.

[24] D Balenson, D Carman, P Dinsmore, and P Kruus. Communications security architecture for army sensor networks. *NAI Labs TR# 00-016*, 30, 2000.

[25] Lidong Zhou and Zygmunt J Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[26] Adrian Perrig, Robert Szewczyk, JD Tygar, Victor Wen, and David E Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[27] David W Carman, Peter S Kruus, and Brian J Matt. Constraints and approaches for distributed sensor network security (final). *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, 1:1, 2000.

[28] Wazir Zada Khan, Mohammed Y Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang. Detection and mitigation of node replication attacks in wireless sensor networks: A survey. *International Journal of Distributed Sensor Networks*, 2013.

[29] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie. Random-walk based approach to detect clone attacks in wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 28(5):677–691, 2010.

[30] Arvind Seshadri, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. Swatt: Software-based attestation for embedded devices. In *Proceedings. 2004 IEEE Symposium on Security and Privacy, 2004*, pages 272–282. IEEE, 2004.

[31] Joseph K Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun Wen Wong. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security*, 9(4):287–296, 2010.

[32] Ming Zhang, Vishal Khanapure, Shigang Chen, and Xuelian Xiao. Memory efficient protocols for detecting node replication attacks in wireless sensor networks. In *ICNP 2009 17th IEEE International Conference on Network Protocols*, pages 284–293. IEEE, 2009.

[33] Isaac Amundson and Xenofon D Koutsoukos. A survey on localization for mobile wireless sensor networks. In *Mobile Entity Localization and Tracking in GPS-less Environnments*, pages 235–254. Springer, 2009.

[34] Eylem Ekici, Yaoyao Gu, and Doruk Bozdag. Mobility-based communication in wireless sensor networks. *IEEE Communications*, 44(7):56, 2006.

[35] Sameer Tilak, Vinay Kolar, Nael B Abu-Ghazaleh, and K-D Kang. Dynamic localization control for mobile sensor networks. In *IPCCC 2005.24th IEEE International Performance, Computing, and Communications Conference*, pages 587–592. IEEE, 2005.

[36] Aman Kansal, Arun A Somasundara, David D Jea, Mani B Srivastava, and Deborah Estrin. Intelligent fluid infrastructure for embedded networks. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 111–124. ACM, 2004.

[37] Guangming Song, Yaoxin Zhou, Zhigang Wei, and Aiguo Song. A smart node architecture for adding mobility to wireless sensor networks. *Physical Sensors and Actuators A*, 147(1):216–221, 2008.

[38] Jamal N Al-Karaki and Ahmed E Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6):6–28, 2004.

[39] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, 2(1):1–22, 2004.

[40] Qin Wang, Mark Hempstead, and Woodward Yang. A realistic power consumption model for wireless sensor network devices. In *SECON'06. 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, volume 1, pages 286–295. IEEE, 2006.

[41] Shashidhar Rao Gandham, Milind Dawande, Ravi Prakash, and Subbarayan Venkatesan. Energy efficient schemes for wireless sensor networks with multiple mobile base stations. In *GLOBECOM'03. IEEE Global telecommunications conference, 2003*, volume 1, pages 377–381. IEEE, 2003.

[42] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In *Proceedings of the first ACM conference on Wireless network security*, pages 214–219. ACM, 2008.

[43] Chia-Mu Yu, Chun-Shien Lu, and Sy-Yen Kuo. Efficient and distributed detection of node replication attacks in mobile sensor networks. In *IEEE 70th Vehicular Technology Conference Fall (VTC 2009-Fall), 2009*, pages 1–5. IEEE, 2009.

[44] Xiaoming Deng, Yan Xiong, and Depin Chen. Mobility-assisted detection of the replication attacks in mobile wireless sensor networks. In *IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2010*, pages 225–232. IEEE, 2010.

[45] Yanxiang Lou, Yong Zhang, and Shengli Liu. Single hop detection of node clone attacks in mobile wireless sensor networks. *Procedia Engineering*, 29:2798–2803, 2012.

[46] Xiao-Ming Deng and Yan Xiong. A new protocol for the detection of node replication attacks in mobile wireless sensor networks. *Journal of Computer Science and Technology*, 26(4):732–743, 2011.

[47] Liang-Min Wang and Yang Shi. Patrol detection for replica attacks on wireless sensor networks. *Sensors*, 11(3):2496–2504, 2011.

[48] Wen Tao Zhu, Jianying Zhou, Robert H Deng, and Feng Bao. Detecting node replication attacks in mobile sensor networks: theory and approaches. *Security and Communication Networks*, 5(5):496–507, 2012.

[49] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, and Sy-Yen Kuo. Localized algorithms for detection of node replication attacks in mobile sensor networks. *IEEE*, 2013.

[50] Kwantae Cho, Minho Jo, Taekyoung Kwon, H-H Chen, and Dong Hoon Lee. Classification and experimental analysis for clone detection approaches in wireless sensor networks. 2013.

[51] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, pages 80–89. ACM, 2007.

[52] Bo Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy, and Lingyu Wang. Localized multicast: efficient and distributed replica detection in large-scale sensor networks. *IEEE Transactions on Mobile Computing*, 9(7):913–926, 2010.

[53] Jun-Won Ho, Donggang Liu, Matthew Wright, and Sajal K Das. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. *Ad Hoc Networks*, 7(8):1476–1488, 2009.

[54] Roberto Di Pietro, Luigi V Mancini, Claudio Soriente, Angelo Spognardi, and Gene Tsudik. Catch me (if you can): Data survival in unattended sensor networks. In *Sixth Annual IEEE International Conference on Pervasive Computing and Communications, 2008. PerCom 2008*, pages 185–194. IEEE, 2008.

[55] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang. Statistical en-route filtering of injected false data in sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(4):839–850, 2005.

[56] Lei Yu and Jianzhong Li. Grouping-based resilient statistical en-route filtering for sensor networks. In *IEEE INFOCOM 2009*, pages 1782–1790. IEEE, 2009.

[57] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, and Peng Ning. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In *Proceedings. 2004 IEEE Symposium on Security and Privacy, 2004*, pages 259–271. IEEE, 2004.

[58] Haowen Chan, Adrian Perrig, and Dawn Song. Secure hierarchical in-network aggregation in sensor networks. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 278–287. ACM, 2006.

[59] Jing Deng, Richard Han, and Shivakant Mishra. Security support for in-network processing in wireless sensor networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 83–93. ACM, 2003.

[60] Bartosz Przydatek, Dawn Song, and Adrian Perrig. Sia: Secure information aggregation in sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 255–265. ACM, 2003.

[61] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao. Sdap: A secure hop-by-hop data aggregation protocol for sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 11(4):18, 2008.

[62] Srdjan Capkun and J-P Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications,*, 24(2):221–232, 2006.

[63] Saurabh Ganeriwal, Srdjan Čapkun, Chih-Chieh Han, and Mani B Srivastava. Secure time synchronization service for sensor networks. In *Proceedings of the 4th ACM workshop on Wireless security*, pages 97–106. ACM, 2005.

[64] Xin Hu, Taejoon Park, and Kang G Shin. Attack-tolerant time-synchronization in wireless sensor networks. In *The 27th Conference on Computer Communications, IEEE, INFOCOM 2008*, pages 41–45. IEEE, 2008.

[65] Zang Li, Wade Trappe, Yanyong Zhang, and Badri Nath. Robust statistical methods for securing wireless localization in sensor networks. In *Fourth International Symposium on Information Processing in Sensor Networks, IPSN 2005*, pages 91–98. IEEE, 2005.

[66] Donggang Liu, Peng Ning, and Wenliang Kevin Du. Attack-resistant location estimation in sensor networks. In *Proceedings of the 4th international symposium on Information processing in sensor networks*, page 13. IEEE Press, 2005.

[67] Hui Song, Sencun Zhu, and Guohong Cao. Attack-resilient time synchronization for wireless sensor networks. *Ad Hoc Networks*, 5(1):112–125, 2007.

[68] Kun Sun, Peng Ning, and Cliff Wang. Tinysersync: secure and resilient time synchronization in wireless sensor networks. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 264–277. ACM, 2006.

[69] Polly Matzinger. Tolerance, danger, and the extended family. *Annual review of immunology*, 12(1):991–1045, 1994.

[70] Mark Burgess et al. Computer immunology. In *LISA*, volume 98, pages 283–298, 1998.

[71] Mark Burgess. Automated system administration with feedback regulation. *Softw., Pract. Exper.*, 28(14):1519–1530, 1998.

[72] Mark Burgess. Two dimensional time-series for anomaly detection and regulation in adaptive systems. In *Management Technologies for E-Commerce and E-Business Applications*, pages 169–180. Springer, 2002.

[73] Mark Burgess. Probabilistic anomaly detection in distributed computer networks. *Science of Computer Programming*, 60(1):1–26, 2006.

[74] Wibhada Naruephiphat, Yusheng Ji, and Chalermpol Charnsripinyo. An area-based approach for node replica detection in wireless sensor networks. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 745–750. IEEE, 2012.

[75] Fazirulhisyam Hashim, Kumudu S Munasinghe, and Abbas Jamalipour. A survivability framework for the ngmn: Inspirations from the human immune system. In *IEEE Latin-American Conference on Communications, LATINCOM'09*, pages 1–5. IEEE, 2009.

[76] Fazirulhisyam Hashim, Kumudu S Munasinghe, and Abbas Jamalipour. Biologically inspired anomaly detection and security control frameworks for complex heterogeneous networks. *IEEE Transactions on Network and Service Management*, 7(4):268–281, 2010.

[77] Lingxuan Hu and David Evans. Localization for mobile sensor networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 45–57. ACM, 2004.

[78] David J Malan, Matt Welsh, and Michael D Smith. Implementing public-key infrastructure for sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(4):22, 2008.

[79] M Aslam, Nadeem Javaid, A Rahim, U Nazir, Ayesha Bibi, and ZA Khan. Survey of extended leach-based clustering routing protocols for wireless sensor networks. In *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS)*, pages 1232–1238. IEEE, 2012.

[80] Dawei Xia and Natalija Vlajic. Near-optimal node clustering in wireless sensor networks for environment monitoring. In *21st International Conference on Advanced Information Networking and Applications, 2007. AINA'07*, pages 632–641. IEEE, 2007.

[81] Samer AB Awwad, Chee Kyun Ng, Nor K Noordin, and Mohd Fadlee A Rasid. Cluster based routing protocol for mobile nodes in wireless sensor network. *Wireless Personal Communications*, 61(2):251–281, 2011.

[82] Adriano B da Cunha, Breno R de Almeida, and DC da Silva. Remaining capacity measurement and analysis of alkaline batteries for wireless sensor nodes. *IEEE Transactions on Instrumentation and Measurement*, 58(6):1816–1822, 2009.

[83] Minki Cho, Jason Schlessman, Wayne Wolf, and Saibal Mukhopadhyay. Reconfigurable sram architecture with spatial voltage scaling for low power mobile multimedia applications. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 19(1):161–165, 2011.

[84] Leander B Hörmann, Philipp M Glatz, Christian Steger, and Reinhold Weiss. Energy efficient supply of wsn nodes using component-aware dynamic voltage

scaling. In *11th European Wireless Conference 2011-Sustainable Wireless Technologies (European Wireless)*, pages 1–8. VDE, 2011.

[85] Andreas Köpke, Michael Swigulski, Karl Wessel, Daniel Willkomm, PT Haneveld, Tom EV Parker, Otto W Visser, Hermann S Lichte, and Stefan Valentin. Simulating wireless and mobile networks in omnet++ the mixim vision. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 71. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[86] Karl Wessel, Michael Swigulski, Andreas Köpke, and Daniel Willkomm. Mixim: the physical layer an architecture overview. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, page 78. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[87] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 60. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[88] Fei Xing and Wenye Wang. Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes. In *IEEE International Conference on Communications, ICC'06*, volume 4, pages 1879–1884. IEEE, 2006.

[89] Nitin G Palan and Aditi P Khadilkar. Media access control protocol modelling for mobile sensor network using omnet++-mixim network simulator. *IET*, 2011.