UNIVERSITI PUTRA MALAYSIA

ENERGY TRUST SYSTEM FOR DETECTING SYBIL ATTACKS IN CLUSTERED WIRELESS SENSOR NETWORKS

NOOR SABEEH HUSSEIN

FK 2016 69

ENERGY TRUST SYSTEM FOR DETECTING SYBIL ATTACKS IN CLUSTERED WIRELESS SENSOR NETWORKS

By

NOOR SABEEH HUSSEIN

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

May 2016

DEDICATIONS

In the name of Allah, Most Gracious, Most Merciful
This thesis is dedicated to:
My dearest parents for their unconditional love and support

and

My dearest friend Sarraa, siblings, and family, for their whole-hearted and substantial support

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

ENERGY TRUST SYSTEM FOR DETECTING SYBIL ATTACKS IN CLUSTERED WIRELESS SENSOR NETWORKS

By

NOOR SABEEH HUSSEIN

May 2016

Chair : Fazirulhisyam Hashim, PhD
Faculty: Engineering

Recently, much more attention has been attracted in the wireless sensor networks. It consists of a large number of small sensing self-powered nodes with resource constraints such as limited computing capability, memory, and energy. Hence sensor nodes generally are deployed in the remote and hostile environments; it is challenging to provide security to the sensor nodes. Furthermore, the specific constraints of the wireless sensor network make the problems even more critical. These networks are susceptible to different kinds of attacks like denial of service attacks, sybil attacks, jamming attacks, black/sink hole attacks (dropping and absorbing of the packets), and slandering attacks. However, the sybil attacks pose as a serious threat because it can be a gateway to other attacks like data aggregation, distributed storage, voting, resource allocation, and misbehavior detection. The attack occurs when a malicious node, called sybil node, illegitimately claims multiple fake identities by either fabricating new identities or impersonating existing ones. Therefore, the detection of a sybil attack in the network is very important. However, the existing sybil detection approaches have shortage to suffice for the constraints of WSNs and the nature of sybil attacks. To address these limitations, this thesis utilizes the concept of trust systems to protect the network from sybil attacks by providing multi-level detection which could work in a hierarchical wireless sensor network. For each level of detection, energy trust system was applied. Specifically, 1^{st} level detection in each cluster head and 2^{nd} level detection in the base station. Furthermore, a centralized management scheme was employed. Aggregation was also applied to avoid communication overhead and save energy. The proposed system was evaluated in terms of memory overhead, communication overhead, and consumed energy. Furthermore, the performance overhead and the detection accuracy were carried out through intensive simulations, as well as extensive comparison with other trust approaches (LDTS and GTMS). The results from the evaluation indicate that the proposed energy trust system for the detection of sybil attacks can provide fast and effective detection as

shown by the true and false positive rates. It showed more than 70% true positive rate and less than 30% false positive rate at the 1^{st} level of detection. For the 2^{nd} level of detection it showed better performance reach to 100% true positive. Moreover, the proposed system was introduced light overhead and storage.

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

SISTEM KEPERCAYAAN TENAGA UNTUK MENGESAN SERANGAN SYBIL DALAM RANGKAIAN SENSOR TANPA WAYAR BERKELOMPOK

Oleh

NOOR SABEEH HUSSEIN

Mei 2016

Pengerusi: Fazirulhisyam Hashim, PhD
Fakulti : Kejuruteraan

Baru ini, rangkaian sensor tanpa wayar telah menarik banyak perhatian. Ia terdiri daripada sejumlah besar nod sensor kecil kuasa diri dengan kekurangan seperti memori, keupayaan pengkomputeran, dan tenaga yang terhad. Oleh itu nod sensor secara amnya diletakkan pada sekitaran bahaya dan jauh. Situasi ini menjadikan misi untuk mewujudkan keselamatan nod sensor menjadi amat sukar. Selain itu, kekurangan WSN tertentu telah membuat masalah lebih kritikal. WSNs terdedah kepada pelbagai jenis serangan seperti serangan penyesakan, serangan sybil, serangan DoS, serangan lubang hitam (menerap dan mengugurkan bingkisan), dan serangan fitnah. Walaubagaimanapun, serangan sybil menimbulkan ancaman serius kerana ia boleh menjadi get laluan kepada serangan lain seperti pengagregatan data, storan teragih, perundian, peruntukan sumber, dan pengesanan tindakan tidak wajar. Ia berlaku apabila nod berniat jahat, yang dipanggil nod sybil, mendakwa pelbagai identiti palsu secara tidak sah sama ada dengan mereka-reka identiti baru atau menyamar sebagai nod yang sedia ada. Oleh itu, pengesanan serangan sybil adalah amat penting dalam WSN. Malangnya, skim pengesanan serangan sybil yang sedia ada tidak berkemampuan untuk mengatasi kekurangan WSN dan sifat serangan sybil. Bagi menangani batasan asas tersebut, karya ini menggunakan konsep sistem kepercayaan untuk melindungi WSNs dari serangan ini. Ia mencadangkan supaya menyediakan sistem pengesanan pelbagai peringkat, yang berkesan untuk WSN berhierarki, sistem kepercayaan tenaga akan digunakan bagi setiap peringkat. Khususnya, pengesanan peringkat 1 dijalankan pada setiap kepala berkelompok, pengesanan peringkat 2 dijalankan pada setiap tapak stesen. Tambahan pula, skim pengurusan terpusat telah digunakan. Selain itu, pengagregatan digunakan untuk mengelakkan overhed komunikasi dan menjimatkan tenaga. Skim yang dicadangkan telah dinilai dari segi overhed memori, overhed komunikasi, dan penggunaan tenaga. Tambahan pula, prestasi overhed dan ketepatan pengesanan telah dijalankan melalui simu-

lasi intensif, dan juga perbandingan terperinci dengan skim-skim yang dipercayai (LDTS dan GTMS). Hasil daripada penilaian ini menunjukkan bahawa pengesanan sybil yang berdasarkan sistem kepercayaan tenaga yang dicadangkan dapat mencapai pengesanan dengan cepat dan berkesan (kadar positif palsu dan benar). Ia telah menunjukkan lebih daripada 70% kadar positif benar dan kurang daripada 30% kadar positif palsu pada pengesanan peringkat 1. Bagi pengesanan peringkat 2, pretasi kadar positif benar telah meningkat dan mencapai 100%. Manakala, sistem yang dicadangkan telah memperkenalkan overhed dan storan yang ringan.

ACKNOWLEDGEMENTS

I would like to express my deep 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 quality of the dissertation.

Furthermore, I am very grateful to the members of my supervisory committee, Assoc. Prof. Dr. Aduwati Sali and Dr. Fakhrul Zaman Bin Rokhani for their help and support for the completion of this thesis. Lastly, I would like to appreciate the department staff and my research group fellows for their assistance during my research and thesis writing.

I certify that a Thesis Examination Committee has met on 06 May 2016 to conduct the final examination of Noor Sabeeh Hussein on her thesis entitled "Energy Trust System for Detecting Sybil Attacks in Clustered Wireless Sensor Networks" 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 Master of Science.

Members of the Thesis Examination Committee were as follows:

Abd. Rahman Bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Syed Abd Rahman Al-Haddad B Syed Mohamed, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

R. Badlishah Bin Ahmad, PhD
Professor
School of Computer and and Communication Engineering
Universiti Malaysia Perlis
(External Examiner)

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

Date: 28 JUN 2016

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

The members of the Supervisory Committee were as follows:

Fazirulhisyam Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

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

Fakhrul Zaman Bin Rokhani, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG KIM 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.: Noor Sabeeh Hussein, GS37095

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of the 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: _____

Name of Chairman of Supervisory Committee: Fazirulhisyam Hashim, PhD

Signature: _____

Name of Member of Supervisory Committee: Aduwati Sali, PhD

Signature: _____

Name of Member of Supervisory Committee: Fakhrul Zaman Bin Rokhani, PhD

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AP	Access Point
BS	Base Station
CM	Cluster Member
CH	Cluster Head
CSMA	Carrier Sense Multiple Access
DOS	Denial of Service
ETS	Energy Trust System
FFD	Full Function Device
HIDS	Host based Intrusion Detection System
ID	Identity
IDS	Intrusion Detection System
LAN	Local Area Network
MAC	Media Access Control
NIDS	Network based Intrusion Detection System
OMNeT++	Objective Modular Network Testbed in C++
OSI	Open System Interconnect
PHY	Physical
PAN	Personal Area Network
QoS	Quality of Service
RFD	Reduced Function Device
SN	Sensor Node
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Overview

Recently, wireless sensor networks (WSNs) have become promising research field which can offer solutions to many monitoring and tracking applications due to their low-date rate, low-energy consumption and short-range link network [1]. WSNs are used in many applications like environment monitoring, health, military sensing, industrial and manufacturing remote control. WSN consists of hundreds or thousands of tiny sensor nodes (SNs)equipped with sensing, computing and communication abilities [2]. Typically, sensor nodes are deployed in remote and hostile environment to monitor physical conditions or a certain phenomenon by sending their readings to the central processing station where the access point (AP) or base station (BS) is responsible for data fusion. However, these sensor nodes have limited computing capability, memory, and energy [3]. A sensor node is a device that translates parameters or events in the physical world into signals that can be measured and analyzed [4]. It consists of four components: sensing unit, processing unit, communication unit, and power unit. The sensing unit is a sensor responsible for measuring a certain data such as natural phenomena or environmental changes. The processing unit collects and processes the signal collected by the sensors. The wireless communication unit transmits the signals from the sensors to the external receiver like a user through the BS. The power unit, usually a battery, is responsible for supplying other units with the required energy to perform their tasks [5].

As WSNs are increasingly implemented in the real world and typically deployed in unattended and hostile regions, they are susceptible to different kinds of attacks such as routing attacks, denial of service (DoS) attacks, and sybil attacks that can reduce the performance of the whole network [6]. Therefore, it is important to give more attention to the security of such kind of networks. However, the scalability and the limited resources make implementing the security solutions challenging. The sybil attack is considered as one of the most aggressive and evasive attacks in sensor networks as it can affect many vital WSN functions, such as voting, routing, data aggregation, fair resource allocation, misbehavior detection, and distributed storage. It succeeds when a malicious node, called the sybil node, illegitimately claims to have multiple IDs and/or location of a legal node [7][8]. Figure 1.1 shows the scenario of sybil attacks in WSN.
In WSN, many methods have been proposed for detecting sybil attack such as resource testing, location/position verification, Registration of the node identities at a central base station, and random key predistribution [9].

Conventional security approaches have been proven to be insufficient to tackle sybil attacks. Recently, a promising mechanism called trust system has come into existence [7][10][11]. Based on past interaction experiences, trust system has been used for assessing the reliability, availability, or security property of a sensor node [3]. In this thesis, the main focus is to initiate a new concept of trust system based on energy for sybil attack detection in WSNs.

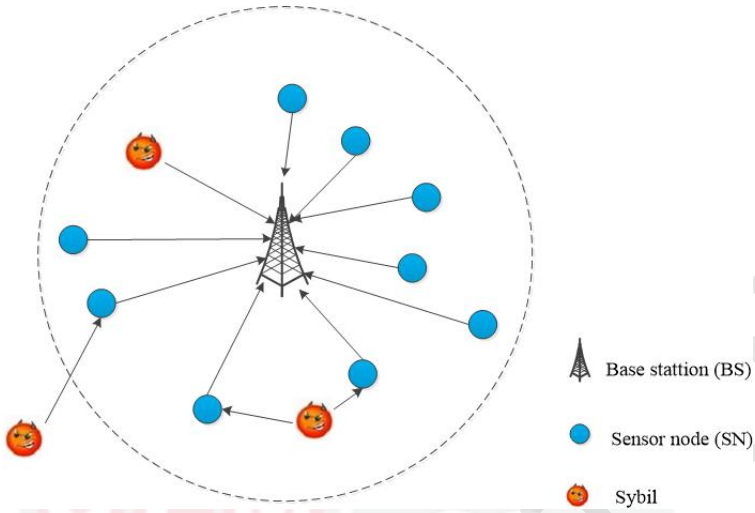

Figure 1.1: Sybil attacks in WSN.

This study focuses on capturing and resolving sybil attack in an effective and timely manner. It considers not only ID and location/position verification, but also the trust detection system by applying multilevel of detection. Unlike most existing trust detection system which is based on past interaction experiences, energy is a metric parameter in this detecting trust system. The proposed multi-level detection framework has two levels of detection. The first level of detection is at the cluster heads level whereas the second level of detection is at the base station. This approach highlights sybil attacks in a dedicated SN or part of the network, instead of involving the whole network by clustering the network and deploying the detection approach.

1.2 Problem Statement and Motivation

The security of a WSN is more important nowadays. However, the constraints in a WSN such as power and memory make it more difficult to apply security solutions for a WSN. Furthermore, high communication overhead and poor scalability increase the difficulty in providing the security for a flat network topology [12]. Therefore, hierarchical clustering is an effective topology in which providing scalability and reducing energy consumption and communication overhead [13][14]. Thus, increasing the network's lifetime [15]. A sybil node impersonates the IDs or/and locations of other legitimate nodes [8] so that it is hard to be detected from a legal node. Therefore, verification the identity and position is important to prevent sybil attacks. For the different sybil detection strategies, the majority of them do not consider the resource constraints in SNs on the ground when searching for new approaches which consider the nature of sybil attacks in WSNs. Depending on the concerns, a trust system is an effective security mechanism to detect sybil attacks which can combine a high security performance with a low operational cost [11]. By observing various trust systems, it has been noted that

recommendation and feedback are essential to build the majority of the trust system such as LDTS [16] and GTMS [17]. Consequently, a lightweight approach is required to counter attacks in WSNs. Therefore, this thesis aims to develop a lightweight trust system to cope with sybil attacks in WSNs with elimination of the recommendation and feedback between nodes.

1.3 Aims and Objectives

The aim of this study is to propose a lightweight energy trust system (ETS) to protect WSNs from sybil attacks. To achieve this goal, the fulfillment of the following objectives is the crucial part of this thesis:

- To design, implement and simulate a clustered WSN. The network is a platform to apply multi-level detection mechanism in which the verification of (ID and position) for each sensor node, aggregation, and trust algorithms are applied.
- To address and analysis the security performance evaluation (i.e., detection accuracy) in terms of true positive, false positive and false negative rates.

1.4 Thesis Scope

The detection of sybil attacks has improved in WSNs. In this thesis, the proposed method focuses on protecting the network from different security attacks not only sybil attack. To provide security in WSNs, many techniques have been proposed such as radio resource testing, position verification, registration of the nodes identity at a central base station, and random key pre-distribution [9]. However, the trust systems are more practical solution in terms of providing security and saving resources like memory and energy [11]. Generally, all current trust systems are based on time as a threshold parameter. Hence, the focus of this thesis is on proposing a trust detecting system based on energy as a threshold vector. The proposed energy trust system for detecting sybil attacks can provide significant memory and energy saving for a clustered WSN. Furthermore, a special emphasis is placed on protecting the network from dangerous security attacks besides sybil attacks by using multilevel detection mechanism in which the applicability is emphasized by using security metrics of true positive and false positive rate.

The summary of the proposed approach in this thesis is illustrated in Figure 1.2. The solid lines along with the colored boxes denote the direction to achieve the determined objectives. The dashed lines with the white boxes illustrate the research fields in WSNs which are not covered in this thesis.

1.5 Thesis Organization

The thesis structure proceeds as follows:

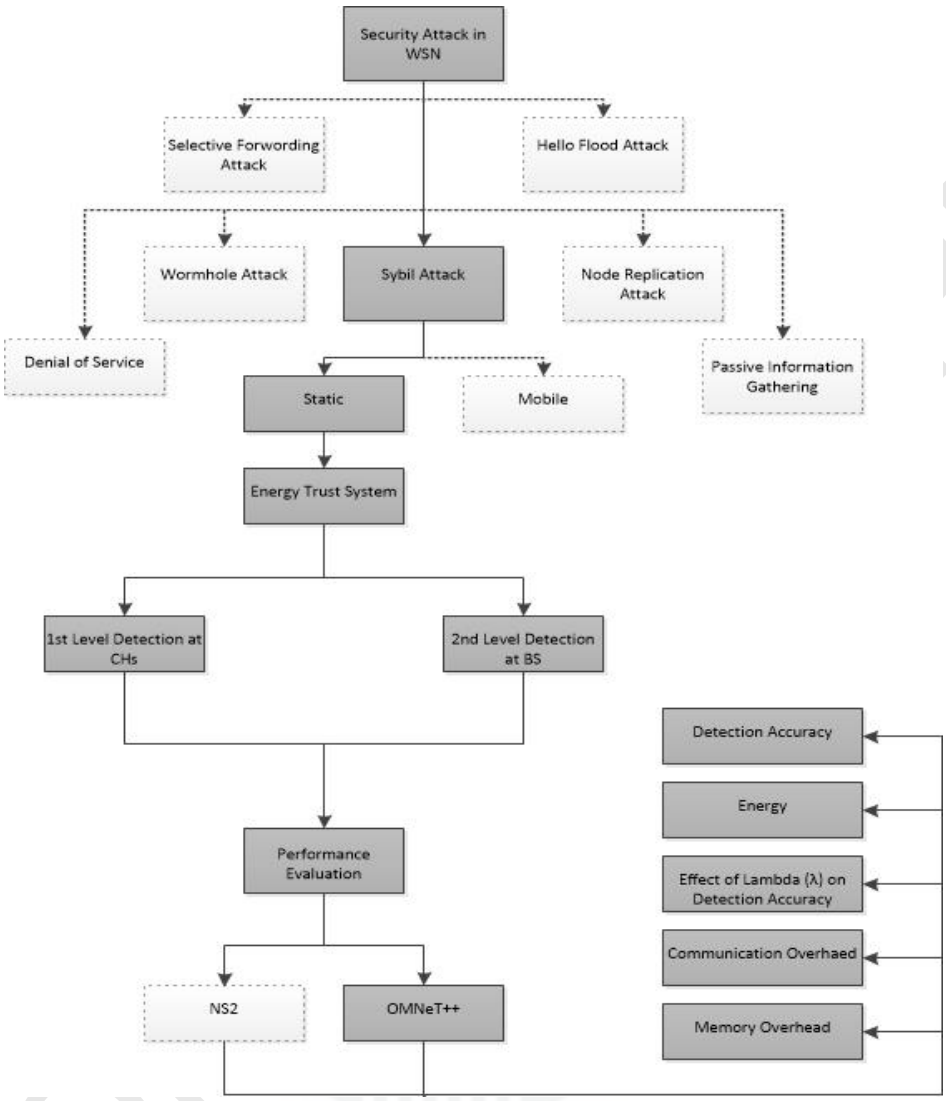

Figure 1.2: Research module.

Chapter 1 presents an introduction and brief overview on sybil attacks in WSNs. This chapter also covers the problem statement, objectives, and scope of the study.

Chapter 2 provides the details about traditional security measures in WSNs. The main focus of chapter 2 is to present the literature review on detecting sybil attacks in WSNs. This chapter highlights the effects of security goals on sybil attacks. It also discusses the challenges that are faced by the designers of the security mechanism to detect sybil attacks. Furthermore, it explains the importance of the trust system as a security solution for WSNs.

In chapter 3, the selected research methodology and processes applied to fulfill the

research objectives described in detail. This chapter also illustrates the two main levels applied to detect sybil attacks in WSNs. Furthermore, OMNeT++ was used to validate the energy detecting system model and the system's components.

Chapter 4 illustrates the simulation results. The outcomes were utilized to evaluate the effectiveness of the multilevel detection system. Respective graphs were used to demonstrate the efficiency in detecting sybil attacks.

Finally, Chapter 5 is the conclusion of the this thesis with the contributions highlighted. Future research directions also were recommended.

REFERENCES

[1] Shuang-Hua Yang and Yi Cao. Networked control systems and wireless sensor networks: theories and applications. *International Journal of Systems Science*, 39:1041–1044, 2008.

[2] Jong-Ha Oh, Sung-Sik Jang, and Tae-Young Byun. A centralized cluster head selection scheme for reducing discrepancy among clusters over wsn. In *Embedded and Multimedia Computing Technology and Service*, pages 699–706. Springer, 2012.

[3] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management*, 9(2):169–183, 2012.

[4] Waltenegus W Dargie and Christian Poellabauer. *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons, 2010.

[5] Neha Jain et al. Energy efficient and cluster based routing protocol for wireless sensor network: A review. *International Journal Of Advance Technology & Engineer Research (IJATER),(November 2011)*, 2011.

[6] Ashfaq Hussain Farooqi and Farrukh Aslam Khan. Intrusion detection systems for wireless sensor networks: A survey. In *Communication and networking*, pages 234–241. Springer, 2009.

[7] Zorana Banković, David Fraga, José M Moya, Juan Carlos Vallejo, Álvaro Araujo, Pedro Malagón, Juan-Mariano de Goyeneche, Daniel Villanueva, Elena Romero, and Javier Blesa. Detecting and confining sybil attack in wireless sensor networks based on reputation systems coupled with self-organizing maps. In *Artificial Intelligence Applications and Innovations*, pages 311–318. Springer, 2010.

[8] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang. Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 24(2):247–260, 2006.

[9] A Perrig, J Newsome, E Shi, and D Song. The sybil attack in sensor networks: Analysis and defenses. In *Third International Symposium on Information Processing in Sensor Networks*, 2004.

[10] Haiguang Chen, Huafeng Wu, Jinchu Hu, and Chuanshan Gao. Event-based trust framework model in wireless sensor networks. In *Networking, Architecture, and Storage, 2008. NAS'08. International Conference on*, pages 359–364. IEEE, 2008.

[11] Tanveer Zia, Md Zahidul Islam, et al. Communal reputation and individual trust (crit) in wireless sensor networks. In *2010. ARES'10 International Conference on Availability, Reliability, and Security*, pages 347–352. IEEE, 2010.

[12] Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su, and Chung-Han J Chen. Weighted trust evaluation-based malicious node detection for wireless sensor networks. *International Journal of Information and Computer Security*, 3 (2):132–149, 2009.

[13] Ossama Younis and Sonia Fahmy. Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *Mobile Computing, IEEE Transactions on*, 3(4):366–379, 2004.

[14] Dali Wei, Yichao Jin, Serdar Vural, Klaus Moessner, and Rahim Tafazolli. An energy-efficient clustering solution for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 10(11):3973–3983, 2011.

[15] Dilip Kumar, Trilok C Aseri, and RB Patel. Eehc: Energy efficient heterogeneous clustered scheme for wireless sensor networks. *Computer Communications*, 32(4):662–667, 2009.

[16] Xiaoyong Li, Feng Zhou, and Junping Du. Ldts: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 8(6):924–935, 2013.

[17] Riaz Ahmed Shaikh, Hassan Jameel, Brian J d'Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 20(11):1698–1712, 2009.

[18] Kashif Kifayat, Madjid Merabti, Qi Shi, and David Llewellyn-Jones. Security in wireless sensor networks. In *Handbook of Information and Communication Security*, pages 513–552. Springer, 2010.

[19] Shital Patil and Sangita Chaudhari. Dos attack prevention technique in wireless sensor networks. *Procedia Computer Science*, 79:715–721, 2016.

[20] Yunxia Chen, Qing Zhao, Vikram Krishnamurthy, and Dejan Djonin. Transmission scheduling for optimizing sensor network lifetime: A stochastic shortest path approach. *IEEE Transactions on Signal Processing*, 55(5):2294–2309, 2007.

[21] Neelam Srivastava. Challenges of next-generation wireless sensor networks and its impact on society. *arXiv preprint arXiv:1002.4680*, 2010.

[22] S. Goyal, T. Bhatia, and A.K. Verma. Wormhole and sybil ttack in wsn: A review. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*, pages 1463–1468, March 2015.

[23] Manish M Patel and Akshai Aggarwal. Security attacks in wireless sensor networks: A survey. In *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, pages 329–333. IEEE, 2013.

[24] Arif Mahmood and Ali Hammad Akbar. Threats in end to end commercial deployments of wireless sensor networks and their cross layer solution. In *Information Assurance and Cyber Security (CIACS), 2014 Conference on*, pages 15–22. IEEE, 2014.

[25] Jaydip Sen. Routing security issues in wireless sensor networks: Attacks and defenses. *arXiv preprint arXiv:1101.2759*, 2011.

[26] Guangjie Han, Jinfang Jiang, Wen Shen, Lei Shu, and Joel Rodrigues. Idsep: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. *IET Information Security*, 7(2):97–105, 2013.

[27] Sweety Saxena and Vikas Sejwar. Sybil attack detection and analysis of energy consumption in cluster based sensor networks. *International Journal of Grid and Distributed Computing*, 7(5):15–30, 2014.

[28] Santhi B. Abirami, K. Sybil attack in wireless sensor network. *International Journal of Engineering and Technology(IJET)*, 10(2):49–53, 2013.

[29] Mirali Khanderiya and Mital Panchal. A survey on detection of sybil attack in wireless sensor network. 2015.

[30] V Sujatha and EA Mary Anita. Detection of sybil attack in wireless sensor network. 2015.

[31] Nitish Balachandran and Sugata Sanyal. A review of techniques to mitigate sybil attacks. *arXiv preprint arXiv:1207.2617*, 2012.

[32] Madhumathi Rajesh, GR Gangadevi, and Rama Sugavanam. On recognizing id based attacks using environs and beam forming approach for wireless sensor networks. In *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*, pages 1–7. IEEE, 2012.

[33] Brian Neil Levine, Clay Shields, and N Boris Margolin. A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA*, 2006.

[34] Karen Hsu, Man-Kit Leung, and Brian Su. Security analysis on defenses against sybil attacks in wireless sensor networks. *IEEE Journal*, 2008.

[35] Murat Demirbas and Youngwhan Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pages 564–570. IEEE Computer Society, 2006.

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

[37] Hui-Feng Huang. A pairwise key pre-distribution scheme for wireless sensor network. In *Intelligence and Security Informatics*, pages 77–82. Springer, 2008.

[38] Rehana Yasmin, Eike Ritter, and Guilin Wang. An authentication framework for wireless sensor networks using identity-based signatures. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 882–889. IEEE, 2010.

[39] Kyung-Ah Shim, Young-Ran Lee, and Cheol-Min Park. Eibas: An efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad Hoc Networks*, 11(1):182–189, 2013.

[40] Srdjan Čapkun and Jean-Pierre Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1917–1928. IEEE, 2005.

[41] Loukas Lazos, Radha Poovendran, and Srdjan Čapkun. Rope: robust position estimation in wireless sensor networks. In *Proceedings of the 4th international symposium on Information processing in sensor networks*, page 43. IEEE Press, 2005.

[42] Ismail Butun, Salvatore D Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *Communications Surveys & Tutorials, IEEE*, 16(1):266–282, 2014.

[43] Tiranuch Anantvalee and Jie Wu. A survey on intrusion detection in mobile ad hoc networks. In *Wireless Network Security*, pages 159–180. Springer, 2007.

[44] Saidat Adebukola Onashoga, Adebayo D Akinde, and Adesina Simon Sodiya. A strategic review of existing mobile agent-based intrusion detection systems. *Issues in Informing Science and Information Technology*, 6:669–682, 2009.

[45] Md Satria Mandala, Asri Ngadi, A Hanan Abdullah, Sambasiva Rao Baragada, S Ramakrishna, MS Rao, S Purushothaman, Dzulkifli Mohamad, SH Salleh, MS Salam, et al. A survey on manet intrusion detection. 2008.

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

[47] Zakira Inayat, Abdullah Gani, Nor Badrul Anuar, Muhammad Khuram Khan, and Shahid Anwar. Intrusion response systems: Foundations, design, and challenges. *Journal of Network and Computer Applications*, 62: 53–74, 2016.

[48] Sanjeev Gangwar. Mobile ad hoc network: a comprehensive study and survey on intrusion detection. *International Journal of Engineering Research and Applications (IJERA)*, 2(1):607–612, 2012.

[49] Oleg Kachirski and Ratan Guha. Effective intrusion detection using multiple sensors in wireless ad hoc networks. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, pages 8–pp. IEEE, 2003.

[50] Tarek S Sobh. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces*, 28(6):670–694, 2006.

[51] Paul Brutch and Calvin Ko. Challenges in intrusion detection for wireless ad-hoc networks. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pages 368–373. IEEE, 2003.

[52] Roberto Perdisci, Giorgio Giacinto, and Fabio Roli. Alarm clustering for intrusion detection systems in computer networks. *Engineering Applications of Artificial Intelligence*, 19(4):429–438, 2006.

[53] Patrick Albers, Olivier Camp, Jean-Marc Percher, Bernard Jouga, Ludovic Mé, and Ricardo Staciarini Puttini. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. In *Wireless Information Systems*, pages 1–12, 2002.

[54] Wendi B Heinzelman, Anantha P Chandrakasan, and Hari Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4):660–670, 2002.

[55] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, and Abdul Waheed Khan. A secure routing protocol with trust and energy awareness for wireless sensor network. *Mobile Networks and Applications*, 21 (2):272–285, 2016.

[56] A Boukerch, Li Xu, and Khalil El-Khatib. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, 30(11):2413–2427, 2007.

[57] Farruh Ishmanov, Sung Won Kim, and Seung Yeob Nam. A robust trust establishment scheme for wireless sensor networks. *Sensors*, 15(3):7040–7061, 2015.

[58] Efthimia Aivaloglou and Stefanos Gritzalis. Hybrid trust and reputation management for sensor networks. *Wireless Networks*, 16(5):1493–1510, 2010.

[59] Zhiying Yao, Daeyoung Kim, and Yoonmee Doh. Plus: Parameterized and localized trust management scheme for sensor networks security. In *2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 437–446. IEEE, 2006.

[60] Sonja Buchegger and J-Y Le Boudec. Self-policing mobile ad hoc networks by reputation systems. *Communications Magazine, IEEE*, 43(7):101–107, 2005.

[61] Zhaoyu Liu, Anthony W Joy, Robert Thompson, et al. A dynamic trust model for mobile ad hoc networks. In *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*, pages 80–85. IEEE, 2004.

[62] Tyrone Grandison and Morris Sloman. A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4):2–16, 2000.

[63] Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato. A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE*, 98(10):1755–1772, 2010.

[64] Haiguang Chen, Huafeng Wu, Xi Zhou, and Chuanshan Gao. Agent-based trust model in wireless sensor networks. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, volume 3, pages 119–124. IEEE, 2007.

[65] Yenumula B Reddy and Rastko Selmic. Agent-based trust calculation in wireless sensor networks. In *Proc. of. SENSORCOMM: The Fifth International Conference on Sensor Technologies and Applications*, pages 334–339, 2011.

[66] Anna Felkner. How the role-based trust management can be applied to wireless sensor networks. *journal of telecommunications and information technology*, pages 70–77, 2012.

[67] Felix Gomez Marmol and Gregorio Martínez Pérez. Security threats scenarios in trust and reputation models for distributed systems. *computers & security*, 28(7):545–556, 2009.

[68] Wenbo Zhang, Guangjie Han, Yongxin Feng, Long Cheng, Deyu Zhang, Xiaobo Tan, and Lidong Fu. A novel method for node fault detection based on clustering in industrial wireless sensor networks.

[69] Rajani Muraleedharan, Xiang Ye, and Lisa Ann Osadciw. Prediction of sybil attack on wsn using bayesian network and swarm intelligence. In *SPIE Defense and Security Symposium*, pages 69800F–69800F. International Society for Optics and Photonics, 2008.

[70] Krzysztof Piotrowski, Peter Langendoerfer, and Steffen Peter. How public key cryptography influences wireless sensor node lifetime. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pages 169–176. ACM, 2006.

[71] Chalermek Intanagonwiwat, Deborah Estrin, Ramesh Govindan, and John Heidemann. Impact of network density on data aggregation in wireless sensor networks. In *Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on*, pages 457–458. IEEE, 2002.

[72] 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.

[73] Horiya Imane Brahmi. Towards efficient data collection in wsns. In *Proceedings of the 2014 workshop on PhD forum*, pages 11–12. ACM, 2014.

[74] Xiaodong Xian, Weiren Shi, and He Huang. Comparison of omnet++ and other simulator for wsn simulation. In *Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on*, pages 1439–1443. IEEE, 2008.

[75] A. Varga. Omnet++ discrete event simulation system, http://www.omnetpp.org/.

[76] C Mallanda, A Suri, V Kunchakarra, SS Iyengar, R Kannan, A Durresi, and S Sastry. Simulating wireless sensor networks with omnet++. *submitted to IEEE Computer*, 2005.

[77] 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.

[78] A. Varga. Mixim framework, http://mixim.sourceforge.net.

[79] Mumtaz M Ali Al-mukhtar and Teeb Hussein Hadi. Diagnosis of failures in zigbee based wireless sensor networks, 2013.

[80] Dayu He. The zigbee wireless sensor network in medical care applications. In *Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on*, volume 1, pages 497–500. IEEE, 2010.

[81] Meng-Shiuan Pan and Yu-Chee Tseng. Quick convergecast in zigbee beacon-enabled tree-based wireless sensor networks. *Computer Communications*, 31 (5):999–1011, 2008.

[82] Abhinav Valada, David Kohanbash, and George Kantor. Design and development of a wireless sensor network system for precision agriculture. *Robotics Institute, Carnegie Mellon University*, 2010.

[83] Simen Kurtzhals Hammerseth. Implementing rpl in a mobile and fixed wireless sensor network with omnet++. 2011.

[84] Feng Chen and Falko Dressler. A simulation model of ieee 802.15. 4 in omnet+. *6. Fachgespräch Sensornetzwerke*, page 35, 2007.

[85] Ólafur Helgason and Sylvia T Kouyoumdjieva. Enabling multiple controllable radios in omnet++ nodes. In *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, pages 398–401. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[86] Vivek Mhatre and Catherine Rosenberg. Homogeneous vs heterogeneous clustered sensor networks: a comparative study. In *Communications, 2004 IEEE International Conference on*, volume 6, pages 3646–3651. IEEE, 2004.

[87] Rahul C Shah and Jan M Rabaey. Energy aware routing for low energy ad hoc sensor networks. In *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, volume 1, pages 350–355. IEEE, 2002.

[88] Anna Hac. *Wireless sensor network designs*. John Wiley & Sons New York, 2003.

[89] Siva D Muruganathan, Daniel CF Ma, Rolly Bhasin, Abraham O Fapojuwo, et al. A centralized energy-efficient routing protocol for wireless sensor networks. *Communications Magazine, IEEE*, 43(3):S8–13, 2005.

[90] Marek Klonowski and MichaB Koza. Countermeasures against sybil attacks in wsn based on proofs-of-work. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 179–184. ACM, 2013.

[91] Hosein Marzi and Arash Marzi. A security model for wireless sensor networks. In *Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2014 IEEE International Conference on*, pages 64–69. IEEE, 2014.

[92] Ibrahim Ammar, Irfan Awan, and Andrea Cullen. Clustering synchronisation of wireless sensor network based on intersection schedules. *Simulation Modelling Practice and Theory*, 60:69–89, 2016.

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

[94] Raquel AF Mini, Antonio AF Loureiro, and Badri Nath. The distinctive design characteristic of a wireless sensor network: the energy map. *Computer Communications*, 27(10):935–945, 2004.

[95] xbow. http://www.xbow.com/, 2008.