A NEW SINKHOLE ATTACK DETECTION ALGORITHM FOR RPL IN WIRELESS SENSOR NETWORKS (WSN)

MOHAMMED QASIM ALI

A project report submitted in partial
fulfillment of the requirement for the award of the
Degree of Master of Electronic Engineering with Honours

Faculty of Electrical and Electronic Engineering
University Tun Hussein Onn Malaysia

JUNE 2019

ACKNOWLEDGMENT

Thank God and help him to complete this research.

I would like to express my gratitude to my supervisor Dr. Ansar Bin Jamil for his continuous help, whenever the road is darkened in front of me I resorted to him and whenever I despair in myself planted hope to go forward and whenever I asked for the knowledge, he provided me and whenever I asked for a quantity of his precious time he gave it to me though His multiple responsibilities.

To whom God has given glory and glory ... To those who taught me tender without waiting ... To whom I carry his name with all pride ... I ask God to extend in your age to see the fruits have come harvested after a long waiting and will remain you stars I promise today and tomorrow and forever. .my dear father. To my angel in life ... to the meaning of love and to the meaning of compassion and dedication ... To the smile of life and the secret of existence to the invitation was the secret of my success and affection my dear mother... To my brother and my companion this life, with you I will be without you I will be like Nothing my brother. To my angel in life, my spirit, and my master, to which the heart beats... My love and dear wife. For those who light my life and make me happy... my kids.

ABSTRACT

With the continuous improvement of science and technology, wireless sensor network technology has gradually been widely used, and provides great convenience for people's living, but with the continuous improvement of the degree of application, wireless sensor network security issues also enter people's field of vision. Sensor nodes can be used for continuous sensing, event recognition and event identification. 6LoWPAN plays an important role in this convergence of heterogeneous technologies, which allows sensors to transmit information using IPv6 stack. Sensors perform critical tasks and become targets of attacks. Sinkhole attack is one of the most common attacks to sensor networks, threatening the network availability by dropping data or disturbing routing paths. RPL is a standard routing protocol commonly used in sensor networks. Therefore, this research presents the works in designing and developing Secured-RPL using the eave-listening concept (overhearing) to treating sinkhole attack. The suggested mechanism method could determine transmitted packages then overhear to the received packet, meaning that the node can overhearing to the neighbor node. Furthermore, three different simulation scenarios were applied, which are the scenario without attacker nodes, scenario with attacker nodes and the scenario with attacker and security by using Cooja simulator to Measurement and analysis performance of RPL in terms of packet delivery ratio (PDR) and power consumption over different packet transmission rate. The experimental results show that the proposed recognition method can identify sinkholes attack effectively and with less storage cost under various wireless sensor networks. Where the optimization ratio of the PDR in scenario with attacker node with the security was close to the scenario with a normal node.

ABSTRAK

Dengan peningkatan sains dan teknologi yang berterusan, teknologi rangkaian sensor tanpa wayar secara beransur-ansur telah digunakan secara meluas, dan memberikan keselesaan yang lebih baik untuk kehidupan rakyat, tetapi dengan penambahbaikan berterusan tahap aplikasi, isu-isu keselamatan rangkaian sensor wayarles juga memasuki dalam pemerhatian masyarakat Nod sensor boleh digunakan untuk pengesanan berterusan, pengecaman dan pengenalpastian peristiwa. 6LoWPAN memainkan peranan penting dalam penumpuan teknologi heterogen ini, yang membolehkan sensor untuk menghantar maklumat menggunakan lapisan IPv6. Sensor melakukan tugasan-tugasan kritikal dan menjadi sasaran serangan. Serangan 'sinkhole' adalah salah satu serangan yang paling kerap terhadap kepada rangkaian sensor, mengancam ketersediaan rangkaian dengan membuang data atau menggangu laluan. RPL adalah piawai standard 'routing' protokol yang biasa digunakan dalam rangkaian sensor. Oleh itu, kajian ini membentangkan kerja-kerja dalam merekabentuk dan membangunkan 'Secured-RPL' menggunakan konsep mencuri dengar untuk mengatasi serangan sinkhole. Kaedah mekanisme yang dicadangkan dapat menentukan paket yang dihantar kemudian mencuri dengar paket yang diterima, yang bermakna nod boleh mencuri dengar nod jiran. Selanjutnya, tiga senario simulasi yang berbeza telah digunakan, iaitu senario tanpa nod penyerang, senario dengan nod penyerang dan senario dengan penyerang dan keselamatan dengan menggunakan simulator Cooja untuk Pengukuran dan analisis prestasi RPL dari segi nisbah penghantaran paket (PDR) dan kuasa penggunaan melawan kadar penghantaran paket yang berbeza. Hasil eksperimen menunjukkan bahawa kaedah pengenalan yang dicadangkan dapat mengenal pasti serangan sinkhole secara efektif dan dengan kos penyimpanan data kurang di bawah rangkaian sensor pelbagai wireless. Di mana nisbah pengoptimuman PDR dalam senario dengan

nod penyerang dengan keselamatan adalah hampir dengan senario dengan nod biasa.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

WSNs	*Wireless Sensor Network*
LLN	*Low Power and Lossy Networks*
RPL	*Routing Protocol for LLN*
ERs	*Emergency Responders*
ND	*Neighbor discovery*
POLL	*Routing Over Low power and Lossy networks*
RFC	*Request for Comments*
RREQ	*Route Request packet*
RREP	*Route Reply*
DIO	*DODAG Information Object*
Contiki MAC	*Contiki Medium Access Control*
Contiki OS	*Contiki Operating Systems*
CPU	*Central Processing Unit*
PDR	*Packet Delivery Ratio*
LPL	*Low Power Listening*
LPM	*Low Power Mode*
LPP	*Low Power Probing*
UDGM	*Unit Disk Graph Medium*
ETX	*Expected Transmission Count*
DIS	*DODAG Information Solicitation*
IETF	*Internet Engineering Task Force*
PGIS	*parking guidance and information system*
CSC	*Cooja Simulation Configuration*
LBR	*LoWPAN Border Router*
NPMT	*Neighbor-Passive Monitoring Technique*

CCA	*Clear Channel Assessment*

CHAPTER 1

INTRODUCTION

1.1 Background

Recently, smart sensor progress is promoting the development of wireless sensor networks. WSN is physical and allows micro-sensors to monitor environmental factors like temperature, humidity, mobility, vibration, seismic activity and more. Sensor buttons are small, smart and cheap[1][2][3]4]. The wireless sensor network becomes more and more frequent especially in data sensitive environment. Many sensor networks contain proposed wireless sensor network routing protocols with security goals[5]. These networks are used to calculate individual sensors based on collective network and physical outline attributes and processing capabilities. The sensor nodes work together and deliver the merged data to the primary network control system for further processing and operation. In this regard, these sensors must be able to comply with the collective network functions according to their respective network policies[6][7].

Commonly, the sensor node is a small device that has 3 main parts, a physical data acquisition subsystem of a physical environment, a local data processing subsystem and a processing memory and a wireless communication data sub-system. In addition, the power source provides the power required for the device to perform scheduled tasks. These sources of energy usually include batteries with limited energy estimates. Charging the battery can be impossible or

inconvenient because the node can be used in an environment that is neither prestigious nor unprofessional. On the other hand, sensor circuits must have a long service life to meet the requirements of the application, in many cases it will take a few months or even years[8][9].

The IETF ROLL working group (routing at low value of power and loss networks) provides a new RPL (including wireless network network). RPL is the first routing protocol with IPv6 support for sensor networks. The module protocols make smart routing decisions when performance data affect the exchange of information and carry data packets to other sensor nodes. If routing results are not smart enough, more recycling for each target data is required in the WSN network, which affects power consumption, bandwidth and sensor node processing[10][11]. With a dozen sensors nodes, RPL can route to thousands of devices and support traffic flow from point-to-point, and point-to-point traffic. In addition, RPL's performance at LLN has low data transfer rates and high loss rates due to restrictions such as cutting, limited sensor processing capacity, limited battery capacity, and limited memory. Finally, the RPL routing protocol enables the efficient use of energy from smart devices, calculates sources, provides flexible topology and data routing[12][13][14].

The usage of devices of low power wireless has become very familiar in our life. Security goal is becoming a requirement in the various WSN applications such as healthcare, automobile, military, the solutions of environment where it supports several advantages. The high WSNs provide considerable opportunities in establishing security projects. Designs related to security concept have a important part in transferring information, it has been one of the most significant areas in terms of routing. Approaching routing data and source position causes network security dangers [15].

1.2 Problem Statement

Different network security is always important because it is essential to protect resources and common communications between authorized users. Previously, your device was not connected to the Internet and was not a danger. However, recently, especially in a low-power network environment, there is a security problem in intelligent devices because of shortage of security characteristics. As mentioned above, wireless sensors are low-memory devices, low-speed data management and CPU operation limits. As a result, the effect of a runway attack is that it can be used to initiate another attack and to reduce or change routing information. Because Sinkhole attack is one of the most stringent routing attacks, they create terminal nodes with misleading routing information, remove packets, and override data or transfer selected data. It can cause energy in the surrounding nodes, causing energy gaps in the WSN, and may lead to inappropriate reactions and can be harmful based on the wrong measurements.

This project aims to propose and develop Secured-RPL routing protocol to tackle sinkhole attack. The works include a study of performance of proposed Secured-RPL in term power consumption impact and packet delay ratio for sinkhole attacks that take place in networks. These results will be compared with the existing RPL.

1.3 Objectives

In general, the objectives of the study as the following:

i. To propose and develop a Secured-RPL routing protocol to prevent sinkhole attacks in WSN.

ii. To implement sinkhole attack against RPL using Cooja simulator to illustrate the correlation among PRD and consumption of power.

iii. To assess the performance of the Secured-RPL and the existing RPL for three different simulation scenarios, which are without malicious nodes (attackers), with system with malicious node and with system with malicious node with security in Cooja simulator.

1.4 Scope of Project

To meet the aims of this research, the scope of this research covers is as the following:

i. making review about wireless sensor network, their applications and working of (RPL).

ii. Doing literature review about usage of the previous studies to recognition sinkhole attacks in WSN and RPL.

iii. Study and analysis of the performance of the Secured-RPL and RPL against sinkhole attack. It shall be prevented complicated technical details and processes for providing an obvious and complete outline of the protocol.

iv. Create a basic network configuration that will be used by all simulation scenarios to compare the performance of Secured-RPL and existing RPL routing protocol.

v. Make three different simulation scenarios in Cooja simulator to make a comparative analysis performance of RPL in terms of packet delivery ratio (PDR) and power consumption over different packet transmission rate.

vi. It will be simulating security mechanism to prevent sinkhole attacks in (WSN) by using Cooja simulator.

1.5 Project Outline

In **chapter 1** the background of harmonics in security WSN and RPL is discussed and problem statement is identified. This is followed by project objectives and scope. In **Chapter 2**, which is named "Literature review" this chapter provides an outline of RPL. It additionally signifies to the ideal of the sinkhole and the security threat to, in addition to an introduction to the WSN. The proposed method is explained in **chapter 3**. This covers the project research frame work and steps in carrying out the project work. The block diagrams of the recognition algorithm and system parameters are presented. In **chapter 4** the simulated results are presented and discussed. Three case studies are considered: 1) system without Malicious mode, 2) system with Malicious mode and 3) system with security. Finally, **chapter 5**. Conclusion & Reference This last chapter demonstrates the conclusion and recommendations.

1.6 Summary

In this chapter, introduction to the project has been presented. This includes the background of harmonics, problem statement, project objectives, and the scope of project.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is a brief review of my theoretical concept on the Wireless Sensor Network (WSN) and the RPL protocol for a full comprehension of each aspect of the research. Moreover, the most important part is a description of previous work-related research on the recognition of sinkhole on a protocol RPL. The brief explanation will be explained in the following subtopic.

2.2 Wireless Sensor Networks

Wireless sensor network technology is also called WSN. This is a new type of sensor network technology. This network technology has been applied to all aspects of human normal life, and the daily activities of human beings. Inseparable, such as production, life and other activities are inseparable from the support of sensor network technologies has become an emerging research and development area because of the large number of applications and systems that can become very useful and have led to low-cost, frequent, inefficient, reusable, low-cost development also called sensor nodes as shown in Fig 2.1., WSNs have a variety of features and species that can digest many troubles arising in different scenarios[16]. Wireless Sensor Networks (WSN) have multiple applications that

can be used in a variety of scenarios, from the simplest to the most complex. For critical applications such as an emergency medical monitoring, volcano monitoring, and forest fire recognition [17]. One of the main goals of the WSN is to monitor data in our world. Compared to infrastructure-based networks, WSN actually run in any operating condition, especially when wireless connectivity cannot be established. WSNs are frequently used for discovering, processing, and communicating data about the physical environment of interest. Generally, WSN includes battery powered sensors with computer components, data processing and communication parts. Sensors can be implemented in both controlled and uncontrolled environments where are important fields.

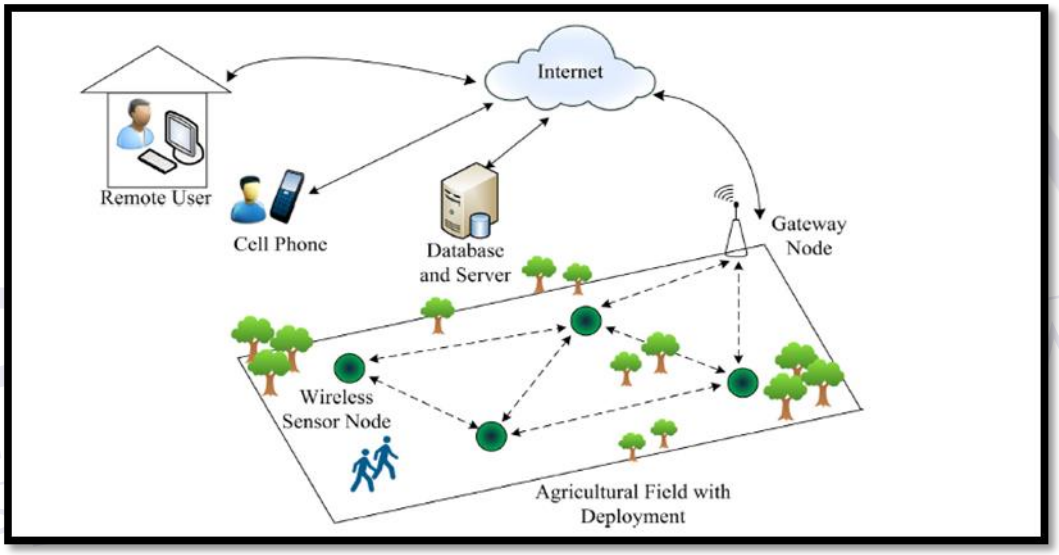

Fig 2.1. Network of Wireless Sensor[18]

2.3 WSN Architecture

Devices field (Sensor nodes) – every sensor node has typically many parts: a radio transceiver with a connection to an external antenna or internal antenna, a microcontroller, an electronic circuit. The Wireless Sensor Networks includes data distribution network and data acquisition network.

i. Interfacing with energy source and a sensor, usually a battery or an embedded form of energy harvesting

ii. the Gate or Access points – A Gateway allows communication among field devices and Host application

iii. Network manager could configure the network, scheduling communication among devices, management of the routing tables and monitoring and reporting the validity of the network

iv. Security Manager could generate, manage and store keys[19].

2.4 Applications of WSN

The WSNS is a free, spatially distributed listener that impresses physical objects or monitors surrounding natural data and collectively delivers data to base stations. The WSN is applied in several areas like agricultural accuracy, animal tracking, natural monitoring, safety and supervision, smart buildings, health care and so on Fig 2.2 shows

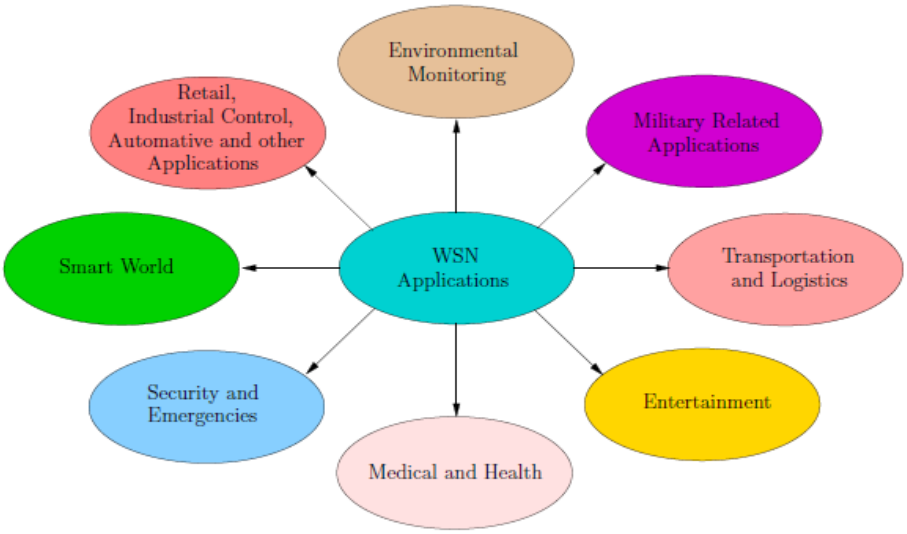

Fig 2.2: Wireless Sensor Network applications[20]

The WSN applications could be categorized as following:

2.4.1 Environmental Monitoring

In this area, the use of WSN is distributed across coal mines, earthquakes, tsunamis, floods, predicted forest fires, gas leakage, storm, rain, water quality, volcanic eruptions, and so on. Since the network identifies and predicts all of the environmental catastrophes in its infancy, it helps to implement security measures at a certain level. Data is recorded with the help of sensors and sent over the Internet to the main station. It helps with caution and helps the public to know about the catastrophic disaster[21] [22].

2.4.2 Smart parking

A smart building has the ability for monitoring and controlling services, based on indoor/outdoor environment and the building structure. The functionalities and features are related to scope of building. one of the most intelligent buildings is smart parking, Given the increase in urban population and traffic congestion, smart parking is normally a strategic problem that ought to pursued not only in study and research, but also in economic fields[23]. Smart parking is a parking system that uses a variety of technologies to effectively manage the garage. Smart parking projects started in many cities. Smart parking is a way for drivers to find effective parking spaces using information and communication technology for outdoor parking. It is also referred to as a parking system, which helps the driver to find a free space using a sensor that detects the presence of the vehicle and ultimately sends the input driver to the space provided. The intelligent parking could be categorized into a parking guidance and information system (PGIS), a traffic data system, a smart payment, electronic parking, many manuals and automatic parking information. every design utilizes various technology for detecting the presence of a vehicle through a slot[24].

2.4.3 Health applications

WSN application could result in significant enhancements in supporting finding-following the emergency responders, sick people monitoring and healthcare [23]. An example to locate and monitor emergency workers can greatly increase support for the organization and administration of real time provision of food and medical sources to human affected by a disaster. This needs efficient communication and processing of data among different ER collections in hostile and remote surroundings. Location, monitoring and communication with ER can be achieved by creating a body sensor system to monitor and monitor rescue teams in hostile and remote environments. Following emergency responders and tracking their important functions with the help of different medical sensors is significant to support the safety of the rescuer. This research is the first step in developing a real time monitoring and tracking system for healthcare professionals. Any alteration in variables such as blood pressure, level of blood oxygen and heart rate of the rescuer could be simply detected and monitored and can be applied to give an alarm when a strange change is noticed[25].

2.4.4 Tracking of automobiles

Vehicle Tracking. Wireless sensor networks are able to enter for auto tracking within a geographic circle. All vehicles / vehicles in large metropolitan areas can contain one or more affixed sensors, which are smart enough to locate, car sizes, street conditions, speeds, densities, etc. When the vehicles approach each other, they replace the brief information. Eventually, these summaries / summaries reach the urban sectors by satellite or the Internet to see traffic status and related information to remote end-users of the investigation. Drivers can also be displayed for erroneous driving conditions and approximate flight times [26].

2.5 Routing procedure

Routing selects the path in a system to transfer information to the destination. In the past, this was defined as directing network traffic. This is one of the most difficult tasks on the network. The type of network in form, has been discussed in telephone networks, electronic networks, wireless sensor networks and transportation networks. Route routes from source to destination through intermediate nodes such as routers and switches.

Routing should be a very important task for them. The data among the base station and the sensor node for laying communication requires routing technology to transmit. Expected data represent the latest research and development in the routing field in WSN. Energy security is lagging behind in advanced routing protocols, and the challenges of dealing with these errors can be overcome. Moreover, since 2013, the proportion of work related to the development of security-based routing protocols has doubled each year[27].

2.5.2 6LoWPAN

The 6LoWPAN idea resulted from the concept that "the Internet Protocol ought to be used to the smallest applications," and that low power applications with restricted processing abilities must have the ability to contribute in the IOT. 6LoWPAN consists of IEEE 802.15.4 power devices and uses the IPV6 address system. It is defined by the IETF. It enables the integration of IPV6 and low-power devices into your personal network. We need this new technology to combine different low-power heterogeneous networks and enable embedded devices to communicate with Internet-based devices. Devices connected to the 6LoWPAN network must send packets and send data. One important term in 6LoPAN is the adjacent search (ND) which allows the nodes to register with routers to ensure effective communication. ND is the basic mechanism for 6LoWPAN used to determine how routers and hosts communicate over the same connection. The IETF ROLL workgroup is currently in the final phase of the RPL

REFERENCES

[1] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design sRequirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.

[2] N. Zaman, L. Tang Jung, and M. M. Yasin, "Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient Routing Protocol," *J. Sensors*, vol. 2016, 2016.

[3] L. Sitanayah, C. Sreenan, and S. Fedor, "A Cooja-Based Tool for Coverage and Lifetime Evaluation in an In-Building Sensor Network," *J. Sens. Actuator Networks*, vol. 5, no. 1, p. 4, 2016.

[4] G. Keerthana and G. Padmavathi, "Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique," vol. 10, no. 3, pp. 41–54, 2016.

[5] D. P. Mirante and H. M. Ammari, "Wireless Sensor Network Security Attacks," *Cris. Manag.*, pp. 25–59.

[6] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Comput. Electr. Eng.*, vol. 66, pp. 274–287, 2018.

[7] M.A. Matin and M.M. Islam, "Overview of Wireless Sensor Network," *Wirel. Sens. Networks - Technol. Protoc.*, no. January 2014, p. 320, 2012.

[8] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[9] I. No and R. Hawi, "Available Online at www.ijarcs.info Wireless Sensor Networks – Sensor Node Architecture and Design Challenges," vol. 5, no. 1, 2014.

[10] M. M. Khan, M. A. Lodhi, A. Rehman, A. Khan, and F. B. Hussain, "Sink-to-Sink Coordination Framework Using RPL: Routing Protocol for Low

Power and Lossy Networks," *J. Sensors*, vol. 2016, 2016.

[11] K. Grgic, D. Zagar, and V. Krizanovic Cik, "System for Malicious Node Recognition in IPv6-Based Wireless Sensor Networks," *J. Sensors*, vol. 2016, 2016.

[12] P. Janani, V. C. Diniesh, and M. J. A. Jude, "Impact of Path Metrics on RPL's Performance in Low Power and Lossy Networks," *2018 Int. Conf. Commun. Signal Process.*, pp. 835–839, 2018.

[13] W. Guo and W. Zhang, "A survey on intelligent routing protocols in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. VII, no. Iv, 2014.

[14] G. Ma, X. Li, Q. Pei, and Z. Li, "A Security Routing Protocol for Internet of Things Based on RPL," *Proc. - 2017 Int. Conf. Netw. Netw. Appl. NaNA 2017*, vol. 2018–Janua, pp. 209–213, 2018.

[15] H. C. Chaudhari and L. U. Kadam, "Wireless Sensor Networks : Security , Attacks and Challenges," vol. 1, no. 1, pp. 859–868, 2011.

[16] M. U. Aftab, O. Ashraf, M. Irfan, M. Majid, A. Nisar, and M. A. Habib, "A Review Study of Wireless Sensor Networks and Its Security," *Sci. Res. Publ.*, no. November, pp. 172–179, 2015.

[17] R. V. Steiner and E. Lupu, "Attestation in Wireless Sensor Networks : A Survey," vol. 49, no. 3, pp. 1–31, 2016.

[18] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Comput. Electron. Agric.*, vol. 118, pp. 66–84, 2015.

[19] V. Kumar, A. Jain, and P. N. Barwal, "Wireless Sensor Networks : Security Issues , Challenges and," vol. 4, no. 8, pp. 859–868, 2014.

[20] H. Yetgin, K. Tsz, K. Cheung, M. El-hajjar, and L. Hanzo, "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks."

[21] V. Hejlová and V. Voženílek, "Wireless Sensor Network Components for Air Pollution Monitoring in the Urban Environment: Criteria and Analysis for Their Selection," *Wirel. Sens. Netw.*, vol. 05, no. 12, pp. 229–240, 2013.

[22] S. R. J. Ramson and D. J. Moni, "Applications of wireless sensor networks — A survey," *2017 Int. Conf. Innov. Electr. Electron. Instrum. Media Technol.*, no. 978, pp. 325–329, 2017.

[23] T. Lin, H. Rivano, and F. Le Mouel, "A Survey of Smart Parking Solutions," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 12, pp. 3229–3253, 2017.

[24] K. Hassoune, "Smart parking Systems:A Survey," *11th Int. Conf. Intell. Syst. Theor. Appl.*, pp. 1–6, 2016.

[25] A. T. Kunnath, P. Pradeep, and M. V. Ramesh, "ER-Track: A wireless device for tracking and monitoring emergency responders," *Procedia Comput. Sci.*, vol. 10, no. 2011, pp. 1080–1085, 2012.

[26] P. Capabilities, "An Overview of Wireless Sensor Networks," vol. 118, no. 5, pp. 1–23, 2014.

[27] A. Sarkar and T. Senthil Murugan, "Routing protocols for wireless sensor networks: What the literature says?," *Alexandria Eng. J.*, vol. 55, no. 4, pp. 3173–3183, 2016.

[28] H. S. R. Babu and U. Dey, "Routing Protocols in IPv6 enabled LoWPAN : A Survey," vol. 4, no. 2, pp. 2–7, 2014.

[29] V. Kumar and S. Tiwari, "Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): A survey," *J. Comput. Networks Commun.*, vol. 2012, 2012.

[30] A. RGHIOUI, A. KHANNOUS, and M. BOUHORMA, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Issues and practical solutions," *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, p. 143, 2014.

[31] W. Dw, *Emerging Technologies in Data Mining*, no. April. Springer Singapore, 2012.

[32] E. Baccelli and M. Philipp, "The P2P-RPL routing protocol for IPv6 sensor networks : Testbed experiments The P2P-RPL Routing Protocol for IPv6 Sensor Networks : Testbed Experiments," no. May, 2014.

[33] Z. Zhang, S. Liu, Y. Bai, and Y. Zheng, "M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks," *Cluster Comput.*, vol. 6, 2018.

[34] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," *2015 Int. Conf. Pervasive Comput.*, vol. 00, no. c, pp. 1–6, 2015.

[35] M. Mascarenhas and P. V. Jain, "A SURVEY ON MECHANISMS FOR DETECTING SINKHOLE ATTACK ON 6LOWPAN IN IOT," no. 1, pp. 134–137.

[36] K. Abirami and B. Santhi, “Sybil attack in Wireless Sensor Network,” vol. 5, no. 2, pp. 620–623, 2013.

[37] M. S. Ahsan, M. N. M. Bhutta, and M. Maqsood, “Wormhole attack recognition in routing protocol for low power lossy networks,” *2017 Int. Conf. Inf. Commun. Technol. ICICT 2017*, vol. 2017–Decem, pp. 58–67, 2018.

[38] J. A. Chaudhry, U. Tariq, M. A. Amin, and G. Robert, “Sinkhole Vulnerabilities in Wireless Sensor Networks,” vol. 8, no. 1, pp. 401–410, 2014.

[39] R. Prajapati and N. Manjhi, “Grid Base Cluster Aproach for Recognition Of Sinkhole Attack in WSN,” vol. 5, no. 17571, pp. 17571–17576, 2016.

[40] A. S. S, M. A. Razzaque, P. Naraei, and A. Farrokhtala, “Recognition of Sinkhole Attack in Wireless Sensor Networks,” no. July, pp. 1–3, 2013.

[41] K. Weekly and K. Pister, “Evaluating Sinkhole Defense Techniques in RPL Networks.”

[42] I. Abdullah, “Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count,” no. February, pp. 50–56, 2015.

[43] F. Zhang, L. Zhai, J. Yang, and X. Cui, “Sinkhole attack recognition based on redundancy mechanism in wireless sensor networks,” *Procedia - Procedia Comput. Sci.*, vol. 31, no. Itqm, pp. 711–720, 2014.

[44] M. Alzubaidi and M. Anbar, “Neighbor-Passive Monitoring Technique for Detecting Sinkhole Attacks in RPL Networks,” pp. 173–182.

[45] A. Dvir, T. Holczer, and L. Buttyan, “VeRA - Version number and rank authentication in RPL,” *Proc. - 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011*, pp. 709–714, 2011.

[46] K. Iuchi, T. Matsunaga, K. Toyoda, and I. Sasase, “Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network,” *2015 21st Asia-Pacific Conf. Commun. APCC 2015*, vol. 4, no. 11, pp. 299–303, 2016.

[47] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, “Recognition of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things,” *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 606–611, 2015.

[48] A. Le, J. Loo, K. K. Chai, and M. Aiash, “A Specification-Based IDS for

Detecting Attacks on RPL-Based Network Topology," 2016.

[49] D. Sheela, "IEEE-International Conference on Recent Trends in Information Technology , ICRTIT 2011 A NON CRYPTOGRAPHIC METHOD OF SINK HOLE ATTACK RECOGNITION IN WIRELESS SENSOR NETWORKS," pp. 527–532, 2011.

[50] C. Thomson, "Cooja Simulator Manual," no. C, pp. 2015–2016, 2016.