ANALYSIS OF NETWORK SECURITY PROBLEMS AND SOLUTIONS FOR MACHINE TO MACHINE COMMUNICATIONS

Abubakar Karabade

Master Thesis

Department of Software Engineering
Supervisor: Assoc. Prof. Dr. Resul DAŞ (F.U.)

JUNE-2016

REPUBLIC OF TURKEY
FIRAT UNIVERSITY
THE INSTITUTE OF NATURAL AND APPLIED SCIENCES

ANALYSIS OF NETWORK SECURITY PROBLEMS AND SOLUTIONS FOR MACHINE TO MACHINE COMMUNICATIONS

MASTER THESIS

Abubakar Karabade

(141137104)

Thesis Submitted Date: **15 June 2016**
Thesis Defense Date: **02 June 2016**

Supervisor: **Assoc. Prof. Dr. Resul DAŞ (F.U.)**
Other members of the jury: **Prof. Dr. Asaf VAROL (F.U.)**
Assoc.Prof. Dr. M. Fatih TALU (I.U.)

June - 2016

DECLARATION

I certify that I read this thesis, and it is fully adequate in scope and quality as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Resul DAŞ
(Supervisor)

Examining Committee Members

Prof. Dr. Asaf VAROL (F.U.)

Assoc. Prof. Dr. M. Fatih TALU (I.U.)

DEDICATION

This thesis is dedicated to my family, I sincerely thank them for their support, encouragement and their endless love, and taught me to work hard.

Abubakar Karabade

ACKNOWLEDGEMENTS

I thank all the people of Elazig, Firat University and those who were associated with this thesis, but it is a worth to especially thank those who were really supportive throughout this thesis. Firstly, I would like to express my gratitude to my master thesis advisor Assoc. Prof. Dr. Resul Daş for his effort, extensive support, and guidance and phase involvement in making this thesis possible. Thanks for his good guidance and advice. I am grateful and pleased to work with him for his inspiration to achieve this thesis. He has always advised me on how to think critically and analytically; especially when it comes to the line of studies, he taught me not to lose hope.

Secondly, I would like to express my gratitude to the Head of Department of Software Engineering Prof. Dr. Asaf Varol, and also thanks to Assoc. Prof. Dr. Bilal Alataş, Department of Software Engineering member, who gave me the excitement about this thesis and continue to provide encouragement; I have learned a lot from their important help.

Thirdly, I would like to thank my thesis committee members for providing the feedback loop of this thesis. Thanks for their advice on my thesis revision. Also, I would like to express my gratitude to all my friends for their excellent advice and encouragement.

Lastly, I thank my parents, sisters, uncles, cousin and brothers for their emotional support throughout my studies and also for their inspiration and prayers.

TABLE OF CONTENTS

Page No

LIST OF FIGURES

Page No

LIST OF TABLES

Page No

LIST OF ACRONYMS AND ABBREVIATIONS

3GPP/4GPP **:** Third generation partnership project
6lowPAN : IPv6 over Low power Wireless Personal Area Networks
ADSL **:** Asymmetric Digital Subscriber Line
ARP **:** Address Resolution Protocol
BGP **:** Border Gateway Protocol
COAP **:** Constrained Application Protocol
CPU **:** Central Processing Unit
DoS/DDoS **:** Denial of Services/Distributed Denial of Service
DHCP **:** Dynamic Host Configuration Protocol
DSL **:** Digital Subscriber Line
DSR **:** Dynamic Source Routing
DTLS **:** Datagram Transport Layer Security
ETSI **:** European Telecommunications Standards Institute
GERAN **:** GSM/EDGE Radio Access Network
GSMA **:** Group Special Mobile Association
GSM **:** Global System for Mobile Communications
HFC **:** Hybrid Fiber Coaxial
HMAC **:** Hash Message Authentication Code
HTTP **:** Hypertext Transfer Protocol
ICMP **:** Internet Control Message Protocol
IEEE **:** Institute of Electrical and Electronics Engineers
IMSI **:** International Mobile Subscriber Identity
IP **:** Internet Protocol
ISP **:** Internet Service Provider
LR-WPAN **:** Low-Rate Wireless Personal Area Network
LTE **:** Long Term Evolution
M2M **:** Machine to Machine
MAC **:** Media Access Control
MQTT **:** Message Queuing Telemetry Transport
OMA **:** Open Mobile Alliance
PLC **:** power line communication

PPP	**:** Point-to-Point Protocol
QoS	**:** Quality of Services
RIP	**:** Routing Information Protocol
RSVP-TE	**:** Resource Reservation Protocol - Traffic Engineering
SCTP	**:** Stream Control Transmission Protocol
SDSL	**:** Symmetric Digital Subscriber Line
SMS	**:** Short Message Service
TCP	**:** Transmission Control Protocol
UDP	**:** User Datagram Protocol
UMTS	**:** Universal Mobile Telecommunications System
UTRAN	**:** Universal Terrestrial Radio Access Network
WAN/LAN	**:** Wide Area Network/Local Area Network
WIMAX	**:** Worldwide Interoperability for Microwave Access
WFA	**:** Wi-Fi Alliance
WLAN	**:** Wireless Local Area Network
WPAN	**:** Wireless Personal Area Network

ABSTRACT

The M2M communication is a rapidly developing large scale networking device which exchanges information and services without human intervention. M2M communication plays a significant role in many applications includes healthcare, smart house, telemetry and intelligent transportation system, etc. creating billions of devices connected to each other virtually and physically through the Internet. In addition, M2M communication supports the development of smart applications that will enhance the demand of people on how to live, work, and exchange information.

Due to the low cost, deployment nature, unguarded, huge number of devices and lack of secure standardization, M2M communication network has several security challenges. These security challenges include Sybil attack, DDoS, falsification attack, etc. Therefore, the intruders try to compromise the credential of network using malware programs and prevent devices from getting services. In order to secure M2M communication network, these security challenges need to be fully addressed to provide confidentiality, availability, integrity and service authentication. In this thesis, we present the analysis of network security problem for M2M communication using OMNET++ simulator and INET simulation model. The analysis is carried out in terms of end-to-end delay, network throughput, sinkhole attack, energy consumption and quality of services (QoS).

This thesis also discusses M2M communication technologies, network security problem, and common existing security solution for M2M communication. In addition, we performed the analysis comparison between the normal network topology and network topology that under attacks. The simulation result shows that when M2M communication network no countermeasure is taken into account, the network can be easily compromised and degrade in its performance.

Keywords: End-to-end Delay, Energy Consumption, Network Throughput, M2M Communication, M2M Network Security, Network Protocols and Architecture, OMNET++ Simulation, Quality of Service.

1. INTRODUCTION

As network operators try to entertain the demand of Internet users, the emergence of new devices such as wired and wireless intensifies the daily routines of Internet users whereby every information could be found on the Internet. Furthermore, technologies like 5G, which have an efficient performance of MAC and physical layers, increase users demand of data [1, 2]. Each and every day, electronic devices are developing such as cameras, printers, smart meters and sensors to monitor the surrounding environment. Therefore, this attracts the attention of network researchers to search and develop new pattern to revolutionize traditional methods of communication for networked devices [3]. The Machine to Machine (M2M) communication is among such paradigms that are needed for emerged next generation technologies which accommodate users' new demands.

M2M communication is a process that allows wireless and wired devices to exchange information without human intervention [4]. The dramatic development of M2M communication embedded devices becomes dominant in communication and communication services. Many significant progressive results are being made such as communication among embedded set of processors, smart sensors, and computer and mobile phone terminals. M2M communication functions by capturing an event and sends it through the network then translates it into meaningful information using the intelligent machine. It provides effective operation like security, smart metering, smart grid, healthcare, industrial monitoring, and automation. Moreover, M2M communication also gives enormous advantages to both business, consumers, as well as mass opportunities to many stakeholders [5]. In general, M2M communication is the fastest growing communication network and the motive behind it is based on two important observations: Firstly, the networked machine is more vulnerable than an isolated one. Secondly, when various machines are interconnected effectively, they can generate an intelligent application.

M2M network enables the communication through a different existing network operator and network infrastructure. Generally, it is composed of a gateway and networked devices. The gateway provides a connection between the devices and area networks. In other words, M2M network uses appropriate technologies for connection depends on the type of application. M2M network has three phases of data processing include collection, transmission, and processing of data. Data collection is the process of collecting data from surrounding environment through a remote sensor and forwarding it to the network.

Therefore, a device like a router, server, and the Internet are used for this purpose [6]. The data assessment delivers collected data from area network to the server. Data processing analyzes the data, interprets the results, and sends it through an application [7]. For example, the machines that are used in industries include a meter, sensor to sense information like the level of inventory, temperature, and performance and sends it through a wireless/wired network.

Due to inexpensive, small payload, a larger number of embedded devices, M2M communications have many standardized interfaces designed to support M2M communication and to provide a framework that enables virtual and real connectivity of the devices. These standardizations include 3GPP, IEEE, GSMA and OMA, WIMAX Forum, WFA, and OneM2M [8]. Moreover, these standardizations provide visualization, designation of modules, and interface of the radio network, remote control, authentication functionality and network functional requirement of end-to-end point. A standard as IEEE has features like lower power consumption, authentication, as well as advanced features like 802.11 and ZigBee. Standard 3GPP/4GPP has features like congestion, overload control, security, and conversion of network device to communication device. Moreover, 3GPP/4GPP has essential features like M2M gateway, group enhancement, network selection and optimization [9]. In addition, it also has new advanced feature like Long-Term Evaluation (LTE) which is used in wireless communication to provide high speed to network terminal and mobile phone. LTE is developed by 3GPP based on UMTS and GSM network technologies [10].

Despite the benefits that M2M communication yields, there are several security challenges that need to be fully addressed. As illustrated in Figure 1.1, these constraints result in difference unique security challenges in M2M communication networks causing difficulty in providing high connectivity, reliability, and efficiencies. This network security problem is becoming a source of serious threats to the expansion of M2M communications users. These threats include Sybil attack, DDOS, falsification attack, etc. This enables attackers to compromise the vulnerabilities of the network through automated malware and sophisticated tools and get access to sensitive data. The techniques that attackers use are so efficient and hard to visualize.

In M2M communication network, network threats need an urgently solution and new defense mechanism systems. In this thesis, we will analyze network security problems and

solutions for M2M communication, with the aim to achieve a solution for network security problems of M2M and threats impact. We will conduct an analysis via simulation, using OMNET++ and INET framework including all seven network layers. In the analysis process, we will deploy many devices connected to the Internet with a control center and intruder attempting to snip the packet. We underline some of the sophisticated strategies of network attacks include gathering information about the system that under attack, energy consumption, and vulnerabilities in order to improve Quality of Service (QoS), end-to-end delay and throughput etc.

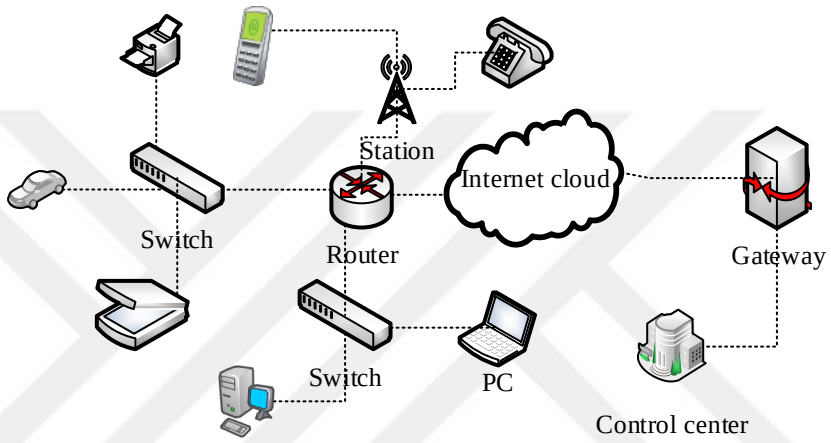

Figure 1.1. M2M communication

This thesis is organized as follows: In chapter 1, we explained the scope and purpose of the thesis. The concepts of M2M communication are introduced. In chapter 2, we present the literature review. Chapter 3 discusses M2M communication technologies enabler such as ZigBee, 6LoWPAN and DSL. In chapter 4, we investigate M2M communication network security problems such as DoS/DDoS attack, falsification of service attack, credentials attack, configuration attacks and leak of service attack. In chapter 5, common existing solutions of network security problems are presented and discussed. This chapter explains essential techniques for securing M2M devices include authentication, key management, and intrusion detection. Chapter 6 discusses the simulation methodology. To evaluate M2M communication network security problem. Hence, in chapter 7, we present the application simulation in details. This chapter explains modules include the IEEE 802.15.4, standard host, access point, Internet cloud and attack module. In chapter 8, we present simulation results, analysis, and comparisons of result metrics like end-to-end delay, energy consumption, and throughput are discussed. Chapter 9 gives the remarks conclusion.

2. LITERATURE REVIEW

Before start explaining the related research work, it is essential to define M2M communication. M2M communication is a fascinating topic, which has been widely discussed in the literature. M2M communication is defined as a process whereby devices exchange an information without human intervention. In another definition, M2M communication refers to the communication between computers, embedded processor, a smart sensor, smart actuators and mobile without human intervention [11]. These definitions are reasonable since M2M communication does not involve human intervention. Here, security is a major threat, which results in environmental damages, failures of the system, financial and data losses. Therefore, analyzing this problem and simulating it is the best way of solving these threats, aiming at providing safety, integrity, availability, reliability and maintainability. In this thesis, we will be studying all of these properties; and in this chapter specifically, we explain the related work.

M2M is an important component of today global network. Diverse of applications realized on M2M communication network for better coverage and low cost. However, the network security problem of M2M has been aggressively addressed by many researchers. In [12], the authors analyzed the effect of discontinuous reception of LTE on the quality of service (QoS) and power consumption. The authors explained the effect of using HTTP traffics and VoIP via simulation. The study was carried out using OMNET++ and SIMLTE which include details of all the network layer models. In the analysis, the factorial method was used which provides qualitative and quantitative impact factors. However, the authors only concentrated on configuration guidelines on mobile wireless of LTE devices, no security issue was considered and evaluated.

In [13], due to the inexpensive and low cost of M2M communication, the authors considered many constraints include little mathematical computation, energy consumption, bandwidth, and storage of home M2M communication network. Firstly, the authors identified some of the fundamental challenges of M2M smart grid network designation to provide better connectivity, reliability, and efficiency. Secondly, the authors proposed an architecture based on three areas includes body areas, personal areas, and local areas of M2M communication network. The authors explained that these areas depend on the application and radios range service for the surrounding environment. Finally, the authors simulated the proposed architecture based on quality of service management and the results showed a demand in resource allocator of home network. However, the authors presented and

proposed the review of smart grid network, but not extensive and exclusive. In addition, the authors did not compare the existing related work.

Recently, the network security problem has been extensively studied and considered as a hot research area in the field of networking. In [14], the authors developed a software and simulation framework which help in analyzing network attacks and defense mechanism. The authors considered an advanced method of network attack include bonnet, distributed denial service attack, and sinkhole attack, etc. and investigated some of the approaches that attackers follow including gathering data about the computer that under attack, the defense mechanism of the system, the integrity of the system and vulnerability assessment. During the environment framework development, three simulation components were defined by the authors which include agent team model (present process includes ontologies team, functionality, classes of agent, protocols), interaction model teams (includes antagonistic model, adaptation, and cooperation) and environmental model which defines the interaction environment. The environment framework was developed with C++ and OMNET++. The result showed better effectiveness and essential defense improvement. However, the work explains network attack simulation framework without any mathematical presentation; and also the work was not implemented and it is limited in component functionalities.

More recently, a fascinating contribution of reliability validating of DoS attacks was proposed in [15] . The objective was to develop an exclusive module of denial of service attacks using OMNET++ simulator. The authors, analyzed the results based on end-to-end delay, throughput, and ratio of packet loss. Result performance works on both simulation model and testbed. In addition, the authors made three contributions: firstly, designation of new extension modules which apply to OMNET++ to enable simulation of wireless QoS attack. Secondly, designation of real-time testbed. Thirdly, benchmarking the obtained results. Moreover, the authors compared simulation results with testbed results to evaluate developed extension module accuracy in case of an excessive load of denial of service attacks. The results showed that denial of service attack compromises and degrades the performance of wireless network. However, the module supports neither generic network failure conditions nor an importance analysis of the devices, defense mechanism, and mathematical presentation.

Another interesting effort on mobile Ad Hoc networks was proposed in [16]. The authors developed a simulation method to analyze network security problems of MANET and attacks effect on performance when dynamic source routing (DSR) protocol is used.

Moreover, the authors focused on performance evaluation of network in terms of end-to-end delay and throughput of ad hoc network. In securing the network, the authors claimed that MANET is a significant component of network functionalities that includes end-to-end packet forwarding which can be easily compromised. The authors explained one of the important areas in routing protocol designation. The authors stated that network security problem is mostly taken into the account in the early stage. The analysis result showed that when no countermeasures are implemented, the network performance is at risk. However, the authors' work only explained routing protocol attack of MANET, without any attack implementation, performance analysis of misbehaving node, and it also lack of benchmarking with existing work.

In [17], the authors explained the security problem of road traffic using VANETs. The aim of the study is to review security challenges of VANET, major types of network attacks, solution to these types of attacks and benchmarking of the results. Moreover, the authors also defined the characteristics and technical challenges of VANET. The review adopted in this work lack merits. In their study, there was consideration of system failure maintainability, safety, integrity, availability, and reliability. In addition, there are many security solutions that have been proposed recently, the authors only described the existing ones without proposing any method, obtaining finding or analysis.

According to recent studies, network security problem is a major challenge in M2M communication network. The structure of Internet itself allows many network security threats to occur. Some researchers proposed that modifying the Internet architecture can reduce threat possibility within the network. There are many studies that focus on improving security of network system include network performance, attacks, quality of service and power. In [18], the authors analyzed recent standards and architecture of M2M communication system. Moreover, the authors realized that most of the developed M2M application would only be vulnerable if proper security was not addressed from the beginning. In tackling network security problems, the authors proposed a unique scheme architecture of M2M communication for establishment of secure connections and performance improvement. The authors explained six communication establishments including bootstrap network, register application, registration of network, and bootstrap service of M2M, connection service of M2M and SCL registration. Even though, the authors explained M2M architecture, but their study did not provide any evaluation and/or

comparison. Moreover, the study did not consider discussing important analysis, mathematical presentation, and defense mechanism.

M2M devices are distributed and operated from different locations. Due to the rapid development of embedded devices, M2M application and service have been increased day by day. Therefore, to achieve user's demand, proper analysis is required to classify network designation problem, security, reliability, network failure, configuration error, large amount of data and congestion. In [19], the authors explained current development of M2M communications network in 4G and advancement towards 5G. The authors considered M2M communication as one of the primary enablers for application and services advancement such as smart grid, hospital, utilities and vehicular. The LTE system advancement, supports the deployment of massive and low-cost devices as well as enhanced network radio access. The authors analyzed the performance based on Long Term Evolution system (LTEs). In their study, they gave the details of system enhancement such as device cost reduction, network coverage, energy efficiency and network control, but they did not provide any evaluation performance of 4G/5G when massive devices are deployed neither did they offer benchmarking with any existing work. Moreover, there was no simulation to support their investigation.

In [20], the authors explained the efficiency of embedded devices and the open challenges whereby a smartphone serves as a gateway (collect a data from sensor nodes). This study provides three contributions: firstly, review of M2M standardization, message queuing telemetry transport (MQTT), architecture and protocols. Secondly, the impact of smartphone as gateway entities. The authors concluded that, in order to reduce the normal time of smartphones battery, it is advisable to maximize collected data from nearby sensors node and interval of transmissions. However, the study did not explore machine to machine communication gateway and data collection mechanism, performance, massive deployment of devices, analysis, and bandwidth and power consumption in details.

The deployment of a massive number of devices enables intruders to exploit the network vulnerabilities using automated malware that may include Denial of Service Attack (DoS), virus, worm, Trojan horse, browser hijacker, rootkits, and botnet etc. In addition, the deployment of a massive number of M2M devices without authentication or key management may result in security challenge compared to Human to Machine (H2M) technologies. In [21], the authors addressed network security problem for M2M communication devices using cloud computing. The main objective was to design a new

cooperation strategy that allows a device to identify an attack before targeting the network. This will enable defense preventive deployment. The authors defined a good architecture which enables transmission of service and data acquisition in cloud computing. However, this study explained M2M, network security problem and proposed architecture, without providing any performance analysis, simulation, and comparison of previous work.

In [22], the author proposed a good network security solution for M2M communication that will reduce the amount of power consumption. Firstly, the author identified the type of network security problem that need more attention and which type of service or entities are threatened. Secondly, the author explained network efficiency and strategies of secure data aggregation that enable a lifetime of the network by optimizing power consumption of the devices. Thirdly, the author proposed authentication method that minimizes the cost of wireless communication channel and prevents network from attack. Fourthly, the author proposed a novel key management protocol to ensure secure communication between the devices. Finally, the author provided analysis using simulation tools. Although, the author explained in details the proposed method, yet it is insufficient to prevent M2M devices from being attacked.

In [23], the authors proposed a way to secure M2M network. The authors explained M2M communication challenges that are not yet addressed due to their low cost, unguarded, massive deployment, and architectures. This study attempted to address new network threats, yet failed to provide any analysis that supports their proposed method.

The main difference between our study and previous attempts is that we analyze network security problem and solution for machine to machine communication. To get better results, performance, QoS, and evaluation, we use a popular and open source OMNET++ simulators and INET framework models. Moreover, we compare the findings with previous studies to provide a benchmark guideline.

3. M2M COMMUNICATION TECHNOLOGIES

M2M communication is a set of devices connected together to allow wired line and wireless to communicate without human interaction. M2M devices resist any overcoming information or load. In M2M communication, information is forwarded through various channels. These channels are a set of devices and applications that enable two or more devices to connect and forward data wired/wireless to each other. Moreover, they also regulate data transmission over a network, error correction, compression, and verification. In this chapter, we explain the most portable technologies used in M2M communication.

3.1 IEEE 802.15.4 Communication Technologies

IEEE 802.15.4 can be defined as a standard used in MAC (Media Access Control) and physical layer for LR-WPAN communication. IEEE 802.15.4 standard was developed in 2003 and is supported by IEEE 802.15 standard. It provides power efficiently, low cost and low data rate for end- to-end communication [24]. IEEE 802.15.4 standard has no upper layer and uses four standards like ZigBee, 6LoWPAN, Wireless HART and MiWi to build network [25]. ZigBee is an IEEE 802.15.4 standard which describes the network layer and application layer. ZigBee is developed by ZigBee Alliance which enables the creation of mesh networks. 6LoWPAN is a basis of IEEE 802.15.4 standard that enables a network to use IPV6 protocol. Wireless HART is a sensor technology that supports multiple vendors and was developed based on HART (Highway Addressable Remote Transducer Protocol). MiWi is set of multiple network protocol and mainly used for home networks to facilitate networked devices such as printer personal computer, Internet gateways, and access point of Wi-Fi and to provide service communication, sharing of data and entertainment.

3.2 Wireless Mesh Networks Technologies

Wireless mesh network technologies are communication technologies used in smart grid. Wireless mesh networks use radio nodes and each node act as independent gateway to create mesh topology. It forms a wireless ad hoc network which consists of mesh devices like router (mesh router sends traffic from source to destination) and gateway (mesh gateway links two or more devices to share information) [26]. It is also known as mesh cloud, which works as a single network. In wireless mesh networks, when nodes communicate with each other and one node is not operating the rest can still work. Moreover, wireless mesh networks support IEEE technologies like 802.16 (IEEE 802.16 is an IEEE standard which defines a set of wireless broadband modules), 802.15 this an IEEE standard, which describes WPAN

(Wireless Personal Area Network) network and 802.11 which describes how devices connect to form mesh network.

3.3 WiMAX Technologies

WiMAX is a communication device uses a wireless network to provide data rate of 72 megabits per seconds. It supports IEEE 802.16 standard that enables broadband access. WiMAX was developed in 2001 June by WiMAX Forum. The recent version supports mesh topology and was designed as substitute to Digital Subscriber Line (DSL) [27]. In addition, the main objective of WiMAX is to transmit about 75 kilometers in line of sight. WiMAX is usually deployed in small settlements (rural areas). In potential applications, WiMAX provides suitable bandwidth connection to various devices, VoIP, IPTV (Internet Protocol Television) and smart grid application.

3.4 Mobile Network

Mobile network is a wireless network and can be distributed within a territory. The mobile network has a base station that provides the service. It also has features like multiple links, less power, and support larger coverage area. Mobile network is a great choice because of the existing current networks. Therefore, most of the companies rely on existing current network infrastructure [28]. It has various generation includes 2G/2.5G, 3G, and LTE. The 2G standard, second generation mobile telecommunications technology, was developed in 1991 to support mobile communication. It enables mobile to transmit more call and has standard like 2.5G and 2.75G. The 3G stands for third generation mobile telecommunication. This standard is an improvement of 2G version. It has features like conversion of the network device to the communication device, M2M gateway, group enhancement, network selection and optimization. It supports wireless network communication and has features like high speed, congestion control, and high downloading rate. LTE is developed based on UMTS, HSPA, EDGE and GSM technologies.

3.5 DSL Technologies

DSL is communication technology that enables high-speed transmission of digital data over telephone network. It deliveres data over a wired telephone line simultaneously. It supports data rates of 100 megabytes per second. In addition, DSL is also divided into two categories including ADSL and SDSL [29]. ADSL stands for Asymmetric Digital Subscriber Line which enables fast transmission over telephone line network and has upstream

bandwidth direction. SDSL, stands for Symmetric Digital Subscriber Line, is a DSL technology that transmits digital over telephone line network and has downstream bandwidth.

3.6 PLC

PLC, stands for Power Line Communication, is wired and wireless communication protocol. It uses electrical wired to transmit data and AC. PLC is mostly used in smart grid healthcare appliance and is operated between 3- 40 MHz [30]. Moreover, PLC devices have restrained themselves in one group of wired and propagation of signal. PLC supports difference frequencies and data rate in different applications.

4. NETWORK SECURITY PROBLEMS

Many conducted researches show that there are several network security problems that are imposed with the use of M2M devices including: Firstly, standardization which is a one of the major challenges that impose network security problem. Even though there are existing standards such as 3GPP, IEEE, GSMA, ETSI, and OMA, but they do not provide efficient security. Secure standardization is required to support the communication. Secondly, data constraint is a biggest challenge in M2M communication network security. In data constraint, the device identifies the data using integrated method or data compression and this results in data handling limitation. Good process is required to handle the data in M2M communication. Finally, user experience and physical attack as a limited user experience results in network security problem. Attackers may exploit M2M communication device through inside and outside threats including rogue's agent, intruder, theft, vandalism and engineer's communication [31]. For this reason, proper security architecture is required to support the M2M communication network. Table 4.1 shows attacks types and categories of network security problems.

Table 4.1. Categories of network security problems

NETWORK SECURITY PROBLEMS		**CATEGORIES**
1. Active threat	DOS/DDOS attack	• Destruction attack • Jamming attack • Exhaustion attack • Hello Flood attack • CAM Table spoofed attack • Sinkhole Attack • Selective forwarding attack • Wormhole attack • Network Protocol Attack
	Falsification of service attack	• Replay attack • Desynchronization attack • Sybil attack • Spoofing attacks
	Credentials attacks	• The credentials attacks involved manipulates of brute force token, verification algorithms, intrusion, and malicious token authentication.
	Configuration attacks	• In configuration attack, the attacker's uses a malicious program like zombies to compromise the internal and external component of network configuration.
2. Passive threat	Leak of service attack	• Tampering attack • Eavesdropping attack • Traffic Analysis attack

Due to low cost and mass deployment, M2M communication devices have more network security problems compared to H2M devices. These network security problems grow rapidly as new technologies are being developed, which enables attackers to exploit network vulnerabilities using automated malware and sophisticated tools. Moreover, most of M2M devices have no password encryption and PIN code. As shown in Table 4.1, we divided the network security problems into two groups includes passive and active threats. The passive threat is a process whereby an attacker tries to learn information about devices but does not disturb network communication. Whereas the active threat is a process that enables attackers to compromise sensor node and get access to the main server.

4.1 DoS/DDoS Attacks

DoS attack is a network security problem that disturbs M2M communication network. DoS attack happens whereby an attacker sends a malicious packet to compromise vulnerabilities of a network service [32]. As illustrated in Figure 4.1, the denial service attack prevents legitimate users from getting access to network component by exhausting the functionality of service and capacity of bandwidth connection [33]. In addition, DoS attacks can be launched indirectly with a lot of compromised devices. Before performing DoS attacks, attackers take control of many computers over a network and all these computers are vulnerable to attack. DDoS attack has many categories including destruction attack, jamming attack, exhaustion attack, hello flood attack, CAM table spoofed attack and sinkhole attack [34].

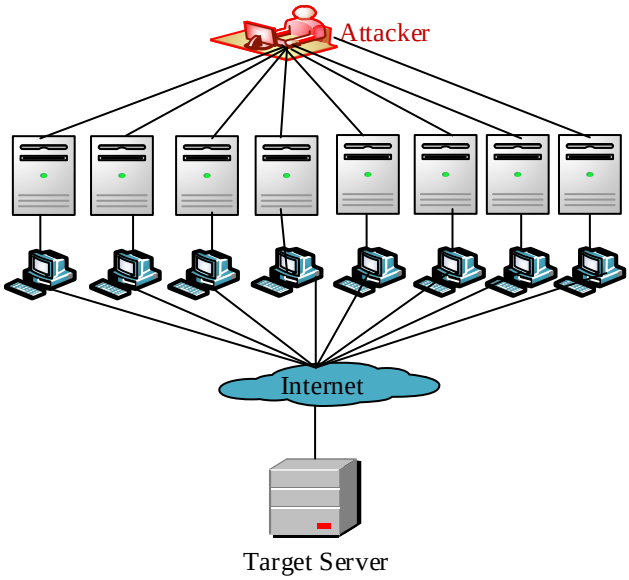

Figure 4.1. DDoS attack

DDoS categories includes:

Destruction attack enables attacker to compromise the vulnerability of a node in order to prevent the device from getting services.

The jamming attack is the process of manipulating a group of nodes which is consistently accomplished by the radio signal transmission. Attackers intentionally can introduce radio signal using Bluetooth or infrared device to jam network signal.

Exhaustion attack involves the disruption of network power. In M2M communication network, the life cycle of the devices has low power which results in deteriorating network performance and makes it easy to attack.

Hello flood attack this type of attacks happens due to query report and devices authentication. This allows an attacker to use query message to target system and intercept packet and cause overwhelming to the network system.

CAM table spoofed the attacker overflows CAM table by turning a switch into a hub. It is done by flooding the CAM table with new MAC addresses of switch port and filling the CAM table beyond its memory capacity. Therefore, the CAM table will no longer deliver packet based on MAC address of switch.

Sinkhole attack is the process of manipulating a node. Attackers rogue a sinkhole and enable themselves to establish a connection to devices root access and create a backdoor on target system.

Wormhole attack this is the type of DDoS attack enables attacker to compromise network gateways and allows them to create wormhole place on multiple nodes to send data [35].

Network Protocol attack is also known as man in the middle attack. Protocol attacks, happens between two people whereby an attacker tries to intercept the network traffic and modify the meaning of data. Network Protocol attack can be performed in many ways. For example, using ICMP protocol to redirect router.

4.2 Falsification of Service Attack

In falsification of service attack, the attacker compromises service and data by falsifying. The attacker here does not disturb gateway service and signal controller, but mainly

intimidates the integrity of network as illustrated in Figure 4.2. Moreover, falsification of service attack sends false packets that have an IP source with an aim to the compromised network [36-39]. As shown in Table 4.1 falsification of service attack has four categories include:

Replay attack is just like ICMP attack whereby an attacker intercepts the flow of message from source to destination. In Replay attack, attackers request broadcast signal with aim of spoofing and consumes the data resources and this causes overwhelming to the network.

Desynchronization attack involves using malicious hardware and software to disrupt the communication between two nodes. In Desynchronization attack, an attacker can limit network time and consume devices resources.

Sybil attack is a botnet attack on a legitimate node. The attacker uses malicious program to recruit multiple nodes and takes control of many nodes, as shown in Figure 4.2. Attackers found it difficult to launch Sybil attack due to every neighboring node communicate with key, but when the attack is launched, routing protocol performance reduce.

Spoofing attack occurs when attackers get to know the IP addresses of a host and attempt of compromising the network using it. In a spoofing attack, the attacker targets forwarding packet to a destination by sending a packet with another host Ethernet address to compromise CAM table entry.

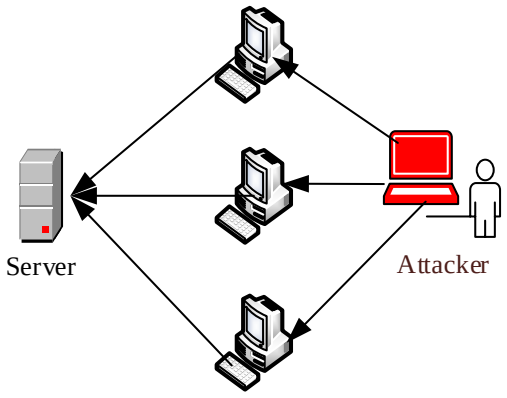

Figure 4.2. Sybil attack

4.3 Leak of Service Attack

Leak of Service Attack is a process whereby an attacker manipulates network data by leaking. Leak of Service Attack does not disturb communication gateway, control signal, data receive, but it increases the frequency of network [40]. There are three categories of leakage of service attack. Firstly, the tampering attack which describes how a network is tempered with. For easy access to network core, the attacker tampers with stored data unit and forces hashed data to recalculate again. Secondly, the eavesdropping attack which describes how an adversary listens to transmission data using malicious program. This type of attack also results in black hole and wormhole attack. Thirdly, traffic analysis attack which specifies how an attacker manipulates sensor node due to consistently flow of traffic.

5. SOLUTIONS TO COMMON NETWORK SECURITY PROBLEMS

As M2M communication market system expands, it encounters significant technical challenges. It sends data simultaneously to the network base station. Similarly, the solution of these vulnerable attacks is complex because it involves in presentation of future where trillions of objects and surrounding environment are connected. The recent development M2M communications are able to detect unusual events such as a damaged device and the change of device location and it also supports M2M device authentication, gateway, monitoring enhancement as well as little security to maintain the entry network procedure. The below clause describes some of existing solutions and countermeasures of M2M communication network security problem that needs to be implemented to prevent the risk and threat.

5.1 Authentication

Authentication is an essential component of secure M2M communication network such as logout, password management, timeouts, remember me, secret question and account update [41, 42]. It is a scheme of communication between the network credential provider and the user interface whereby the user credentials are compared for authorized access. In addition, the authentication allows assurance establishment remotely, locally, enhance trustworthy communication of sensory node data and protect the M2M communication network from falsification of service attacks

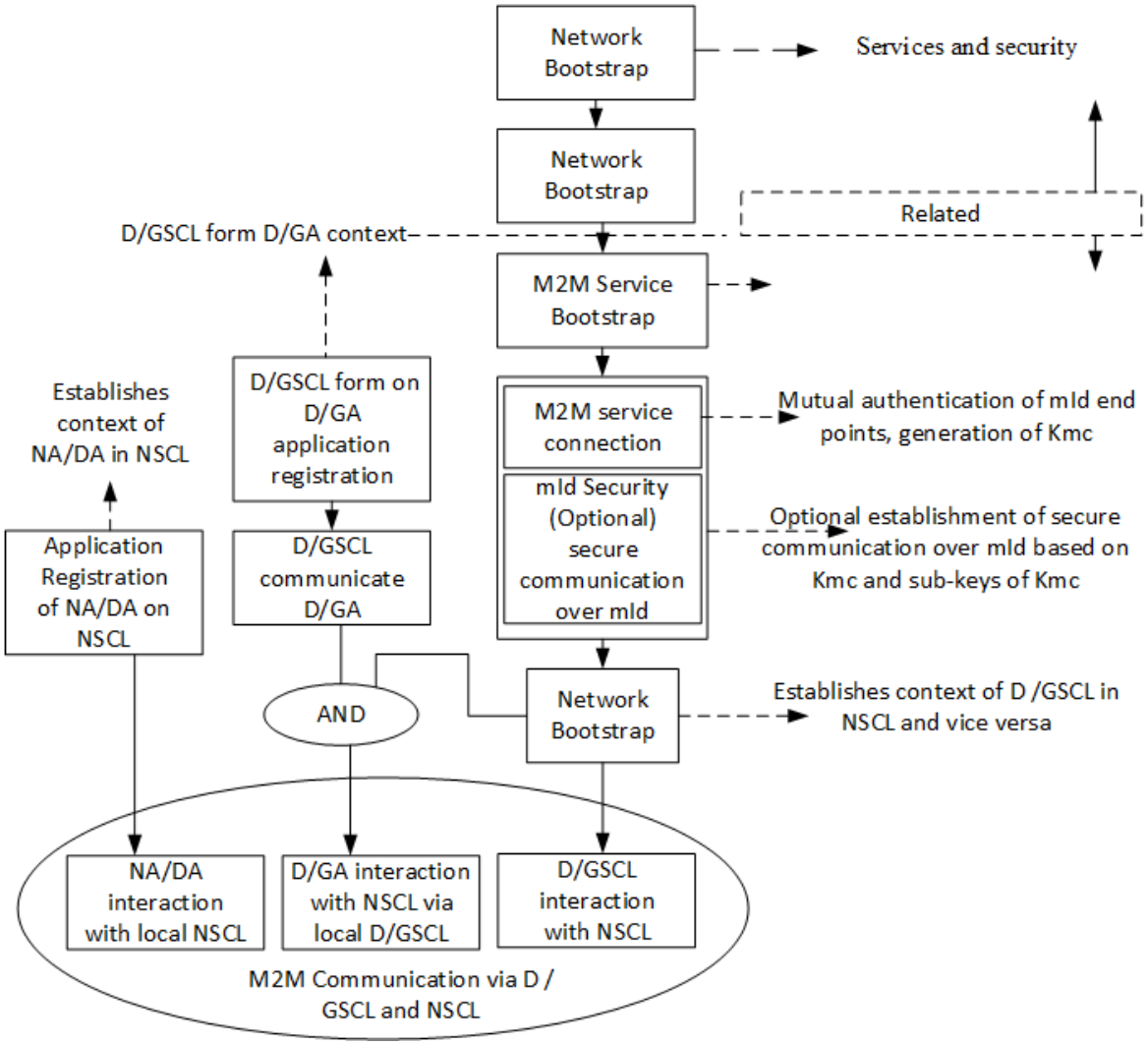

Figure 5.1. Authentication of device in M2M communication

As illustrated in Figure 5.1, the authentication of M2M communication requires a good strategic process to ensure that the network access is secure. It allows M2M gateway devices to register. For example, 3gpp network registration such as UMTS (Universal Mobile Telecommunication System) uses IP address to initialize a mutual agreement on a set of keys. Authentication works hand by hand with verification, confidentiality, integrity, availability and trust management. M2M devices are mostly able to develop trust relationship with one another using cryptographic and non-cryptographic technics such as random pre-shared key, X.509 , raw public key, bootstrap IMSI (International Mobile Subscriber Identity) pre-shared key, SMS authentication, HMAC (keyed-Hash Message Authentication Code), etc.

5.2 3GPP/4GPP

3gpp stands for third generation partnership project, which is an improvement in service, network and system requirements of M2M communication devices. It solves the problem of overloading control, network, and reduction of cost, power optimization, signaling, and security. For example, M2M communication device that has multiple connections to different networks will have the problem of traffic hijacking and signal problem due to limitless in human intervention [43, 44]. The security work group of 3gpp protects the network service remotely from attack and provides trust environment between the devices.

5.3 Key Management

The Security of M2M communication device is unable to provide the traditional demand and protect the network from physical attack. Therefore, key management technic novel approaches were proposed [45]. As shown in Figure 5.2, the key management is a technic that provides a session key (the session key is a unique key generated by network management for end-to-end connection of network devices) which uses symmetric/asymmetric algorithm to communicate remotely with M2M center base server. It provides a strong security chain such as assurance, integrity, and message source, session of communication and data storage as well as protecting the M2M communication devices from malicious attacks.

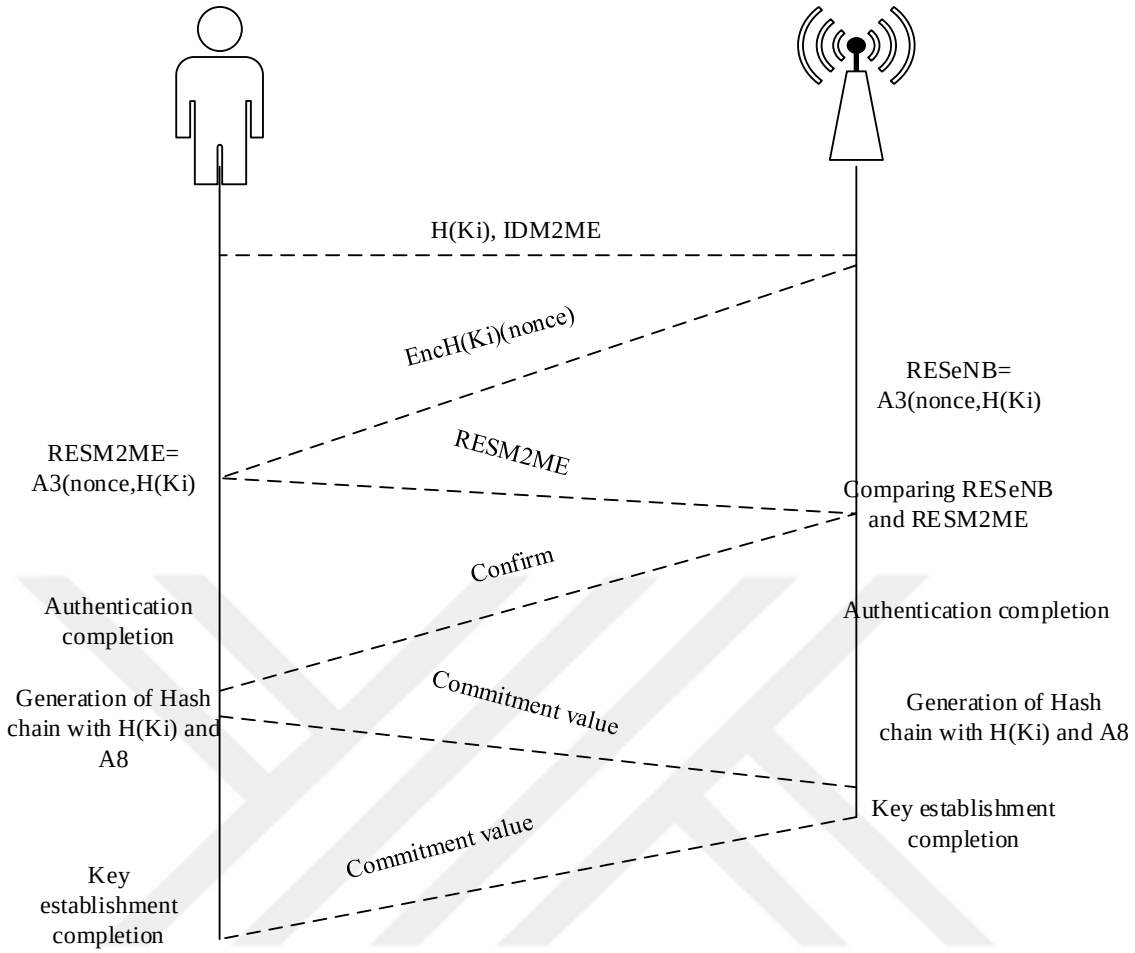

Figure 5.2. Key management of M2M communication device messages exchanges

5.4 Detection

Namely, the increase M2M communication users' number. This gives the attacker an easy way to get access to the system. Intrusion detection is a technic designed to identify unauthorized access and to protect M2M communication network from malicious attack [46]. Since the attack of M2M communication node requires a lot of time, it is advantageous to M2M communication node to monitor one another and detect the compromised node early using all the available data.

5.5 Reply Protection

As the networking system grows, security becomes a major concern in today's world. The challenge is to provide the service to all users in a proper process without teardrop. The attacker can get access to the information easily during the transmission and compromise the credential of the network. For example, in the network management environment, network nodes are distributed and users want to get access to the data that are distributed across the

network; the servers are able to communicate with the user for service request using messages. Therefore, during messages exchange session attacks may occur [47]. The reply protection ensures the security of false reply messages and it also ensures only a piece of information is sent per device.

5.6 IP Security of Network Layer

As shown in Figure 5.3, IP security is a protocol in the network layer. It provides a secure communication from source to destination using authentication and replay messages protection. It uses transportation layer protocol like TCP and UDP [48,49]. IP security services are distributed within all the application that is running on M2M devices for example IPV6. In addition, the IP security ensures integrity, confidentiality of communication.

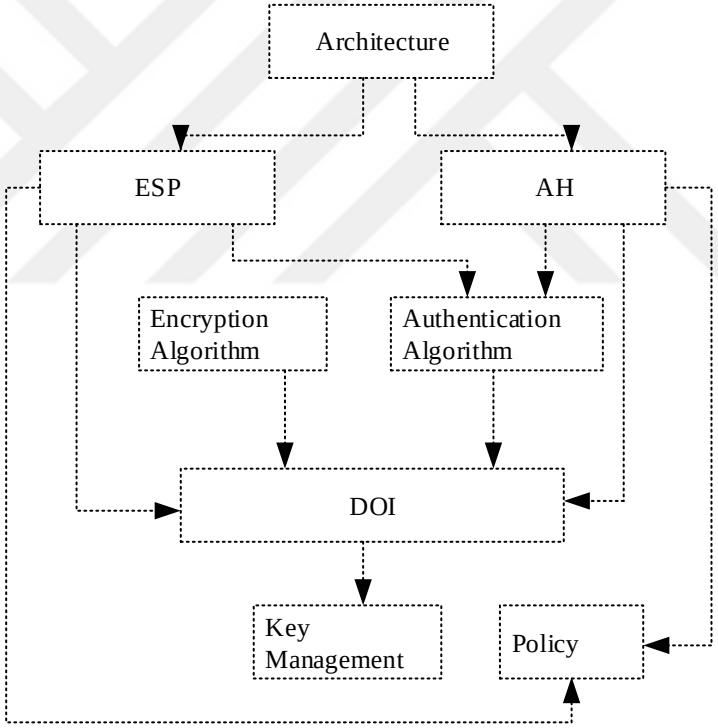

Figure 5.3. IP security of network layer activity diagram

5.7 COAP Security of Transport Layer

Even though IP security can be used in the transportation layer but is not mainly designed for web protocol such as HTTP or COAP. In transportation layer, The DTLS (Datagram Transportation Layer Security) is used to guaranty a secure communication between transportation and application layer [50,51] as shown in Figure 5.4.

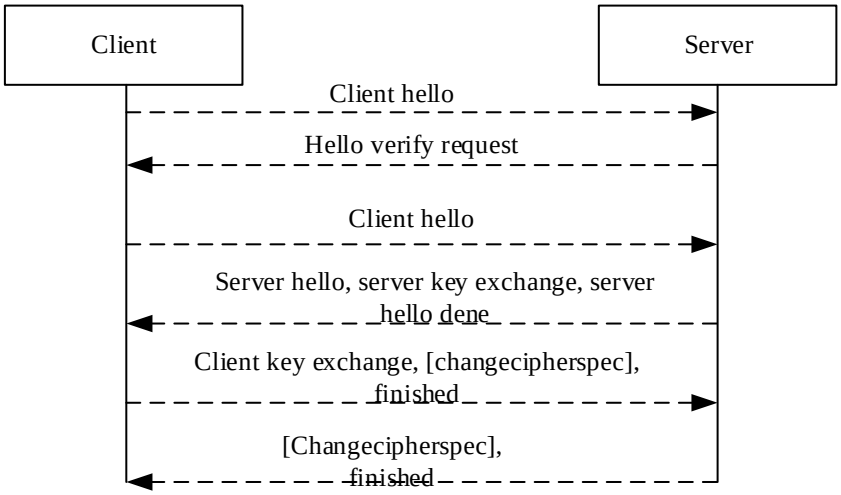

Figure 5.4. COAP security of transport layer messages

5.8 IEE 802.15.4 Security

M2M communication uses IEEE standard for security. These standard include IEEE 802.15.4 security. IEEE 802.15.4 security is a protocol in the link layer which supports 6LOWPAN network [52]. IEEE 802.15.4 security provides security solution of M2M communication network link and it protects the communication node. It uses a single shared key to protect all communication nodes and when a single machine is compromised, the whole security is compromised.

6. METHODOLOGY

The M2M communication is a larger scale networking that can be geographically distributed with different channels of communication technologies. The end user of M2M devices sends huge amounts of data to control remote center. Therefore, due to security problem of M2M communication, it is essential to provide a solution that will prevent the breach of data, connectivity, performance and network failure. In this chapter, we describe the methodology used for the simulation and result analysis.

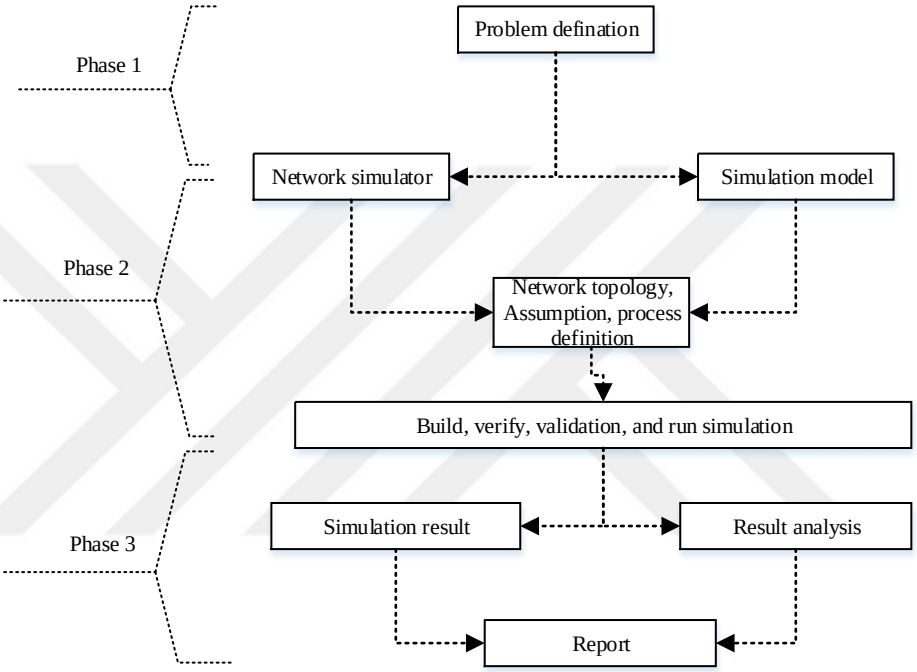

Figure 6.1. Methodology

The objective of this thesis is to analyze the network security problem and to explore potential secure solution for M2M communication. Moreover, in securing M2M communication system, three important dimensions are implied. Firstly, securing the devices and service provider. Secondly, securing exchanged data and communication within the network. Thirdly, securing deployed physical devices and network infrastructure. In order to obtain efficient results and designation, this thesis also includes all OSI models of network to provide the security that will suit all network layers. In addition, we explain that security in M2M communication system as an essential component of network functionalities include packet forwarding and network operation which are easy to compromise if a proper security is not implemented.

The methodology techniques adopted throughout of this work consist of three phases as shown in Figure 6.1. In phase 1, we define the objectives of the study, problem and solution for M2M communication network. Moreover, we review ETSI documentation, GSMA specifications, academic journals, white papers and news articles. Phase 2 consists of network simulator and simulation models for generating network topology, assumption and process definition. In generating network topology, we deploy several numbers of M2M devices in order to verify and validate the effect of network security problem for M2M communication systems, in terms of performance metrics; for example, delay, queue, quality of services, throughput, packet loss, and scalability, by means of OMNET++ simulation tools. Moreover, we set up many parameters to enable comparison of the simulation. Phase 3 offers the analysis of the results when larger numbers of M2M devices are simulated on OMNET++ with INET framework model. The advantage of using OMNET++ is to obtain detailed analysis results. Moreover, the results are normalized and compared in order to obtain a comparative and quantitative analysis.

7. SIMULATIONS OF APPLICATIONS

In early years, network researchers used mathematical and experimental models to verify network feasibility and performance. However, in recent years, due to the rapid revolution of computer network, it is too complicated to analyze the network using mathematical modeling. Network simulator helps researchers to understand network performance, behavior, design testbed and protocols to meet user's requirements. In this chapter, we present network simulator for our analysis, the related modeling assumption (for example, traffic and network models, and devices model).

7.1 Simulator Description

The simulation is carried out using OMNET++ simulator and INET framework. OMNET++ is an open source discrete event simulator used for simulating wired and wireless networks. The motive behind OMNET++ is developing a powerful simulator tool that can help academics, researchers and educationalist. Moreover, it has been free to the public since 1997 and has large number of network research users. OMNET++ simulator unlike other simulators (for example, NS-2, NS-3, j-sim etc.) is not designed only for network simulation, it can also be used for multiprocessors modeling, hardware distribution system and evaluation performance of complex systems. The components of OMNET++ were developed with C++ code. They include all network layers of protocol stack, from application to physical layers. The models use high-level language called NED (Network Description Language), which defines models structure. The distribution of OMNET++ works on both Windows, Mac OS X, Linux, Ubuntu, Fedora, Red Hat, OpenSUSE. OMNET++ has a comprehensive Graphical User Interface (GUI) [53].

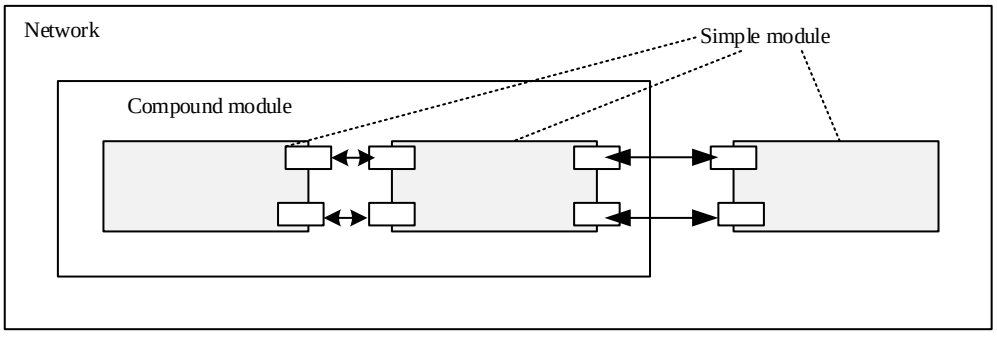

Figure 7.1. Model Structure in OMNeT++

As illustrated in Figure 7.1, OMNET++ has a module; this module is a component based model that forms a network and is able to send/receive messages from other modules. In

OMNET++, a module could be a server, router, host and any component that establishes communication within network. A Module consists of two hierarchical components, namely simple and compound module. Simple module is also known as active module and contains only one component which has its own C++ code. Moreover, simple module allows the definition of comportment algorithm. Compound module is a top-level module that contains one and more sub-modules. In compound module, one or more sub-module can be included to form a compound module and no restriction for adding the nested module. In addition, the channel allows simple and compound module to connect and communicate via messages and gate (Gate can receive and send messages simultaneously) or directly to module destination.

The INET framework is a simulation model library and open source for OMNET++ discrete event simulator. It allows the implementation of protocols stack, network agents, and model. INET framework uses message passing approach to communicate with other modules. Each module describes the network protocols and agent, which can be connected to form switches, host, router etc. When we compare INET framework with OMNE++, OMNET++ uses only generic modules while INET framework is a model for OMNET++. INET framework is frequently used when developing and validating new network protocols. In addition, INET framework contains several protocol implementations such as TCP, UDP, SCTP, IPv4, IPv6, Ethernet, PPP, IEEE 802.11, etc. and several application models. It also allows the implementations of MANET protocols, MPLS, RSVP-TE, difference server and mobility [54]. Therefore, the INET framework is mainly built to support realistic simulation for wired and wireless network.

7.2 System Model

M2M communication is a fast growing communication technology includes devices like vending machine, medical equipment, and smart grid devices. Normally, M2M communication network is similar to WAN/LAN network but it is mostly used for enabling sensors, devices, and control units to communicate and to instruct other devices. As illustrated in Figure 7.2, the general concept of M2M network is to use intelligent devices to create intelligent connection and these devices are monitored remotely. Therefore, the communication involves two stages: firstly, electronic devices and sensors which are attached to remote control machines and depend on appropriate function of machines. Sensors and electronic devices collect data such as temperature, speed from surrounding

environment. The data are transmitted wired/wireless to central server. Secondly, the central remote server analyzes the data into meaningful information and makes initiates decisions for status display. Due to low recurrence update, it is essential that the transmitted messages are well-transmitted between the devices. Moreover, M2M devices can also monitor inventory coolers, on/off building alarm and automatically enable applications to be connected.

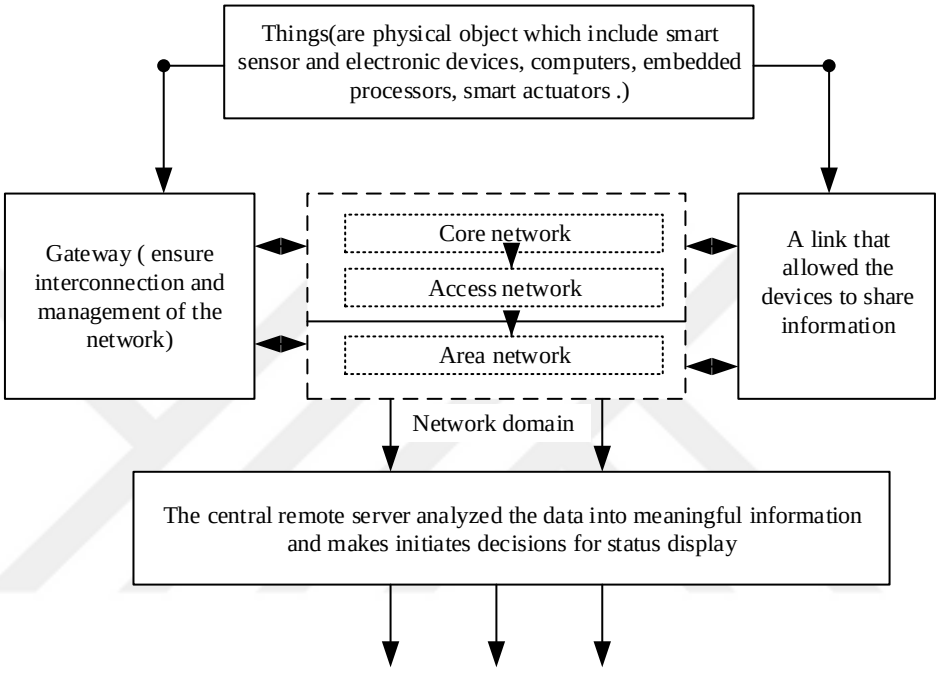

Figure 7.2. How M2M work

As illustrated in Figure 7.2, the existing architecture of M2M communication consists of three interlinked domains: M2M device, network and application domain. Firstly, the M2M device domain describes the devices that sense data from the surrounding environment within a small amount of time for network. Therefore, smart devices and gateways are generated automatically to send a request and reply. Each device is generated by many functions including processing, data acquisition and power. In addition, the gateway ensures interconnection and management of the network. Secondly, network domain which provides the communication between M2M application and M2M device gateways. Figure 7.3 shows that network domain uses network modules such as service and functionality to provide reliable transmission of data through sensory devices. Network domain has two important parts that is M2M area network and M2M access network. M2M area network provides MAC and physical layer connection and also allows M2M device to connect to the network

through a gateway or router. M2M access network allows M2M devices to communicate with a network core including Internet Protocol, xDSL, HFC, satellite, GERAN, UTRAN, e-UTRAN, WLAN, WiMAX. Finally, application domain which consists of middleware/software that forwards data through application services. It has end server that indicates paradigm component of M2M communication. The end server uses data for integration point and also allows data transfer [55].

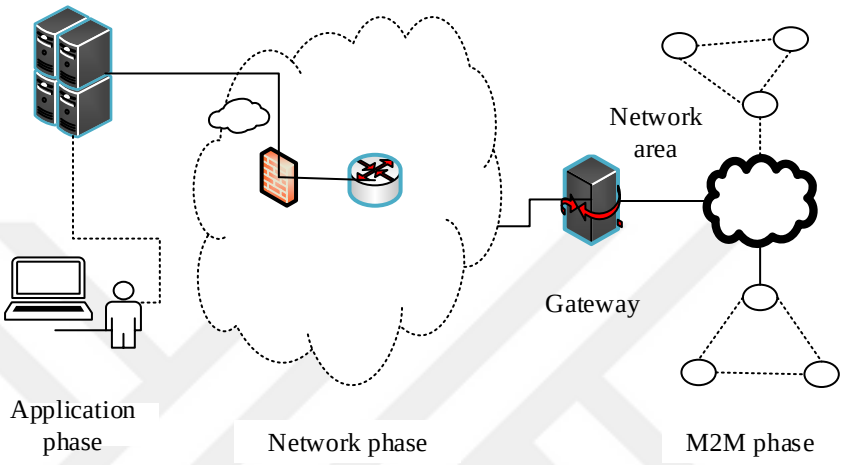

Figure 7.3. Simple architecture of M2M

7.3 Simulated Network Topology

In order to design our network topology, we categorized our topology into three phases: device phase, application phase, and network phase. The network topology that will be used during the simulation can be seen in Figure 7.3 and 7.4. We use such network topologies to analyze network security problem for M2M communication. It is a complex network that contains both wired and wireless nodes (devices). The network consists of 6 routers (one acts as gateway and 5 forward packet filter from source to destination), Internet cloud, remote control center, access point, switch and standard host. IP addresses and routing tables are set up by IPv4 network configurator module. In wireless section, the network consists of IEEE 802.11 scalar radio medium model which uses a scalar method to transmit power in analog interpretation. The devices periodically send UDP packets to the remote center. The packets first arrive at gateway; the gateway will send the packet to remote control center where initiative actions take places such as data collection, data analysis, storage, and decision making.

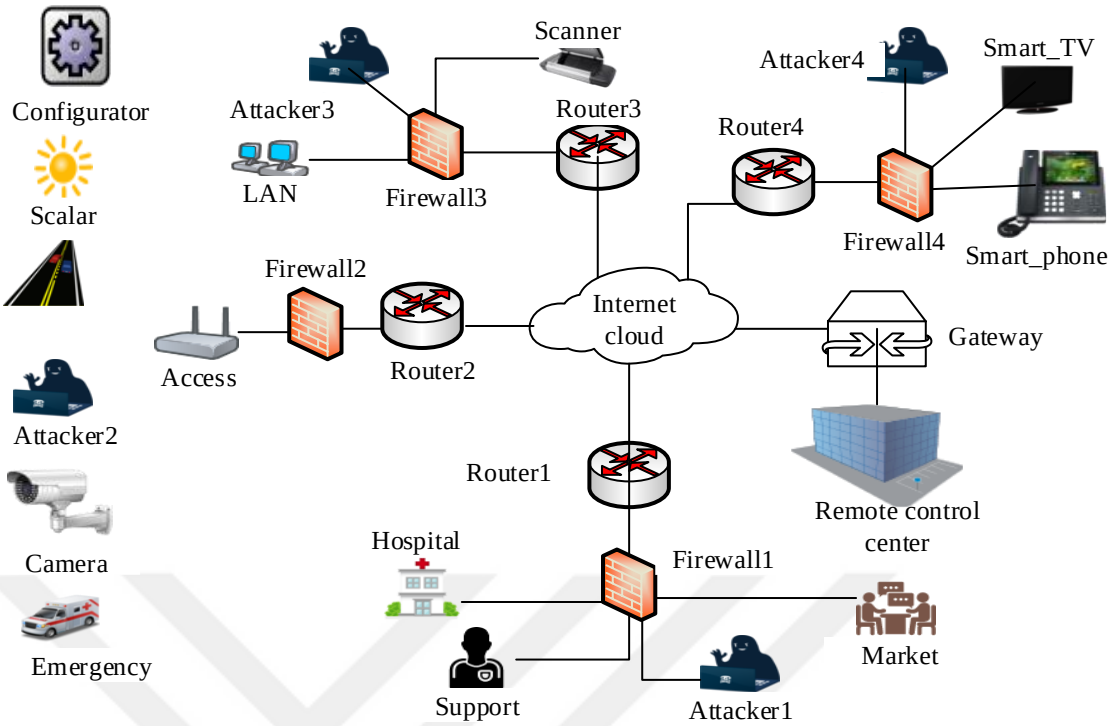

Figure 7.4. Simulated network with attack modules

The description of the devices (nodes) is defined in the modules. We generate a convenient module which acts as OMNET++ classes. These modules receive/send messages from one module to another and the structure of the modules is defined in the network event descriptor (NED). Moreover, a module must have at least one NED file such as simple or compound module. Our simulated network consists of many modules including host, server, attacker and firewall modules. INET simulation model allows us to implement some of the modules.

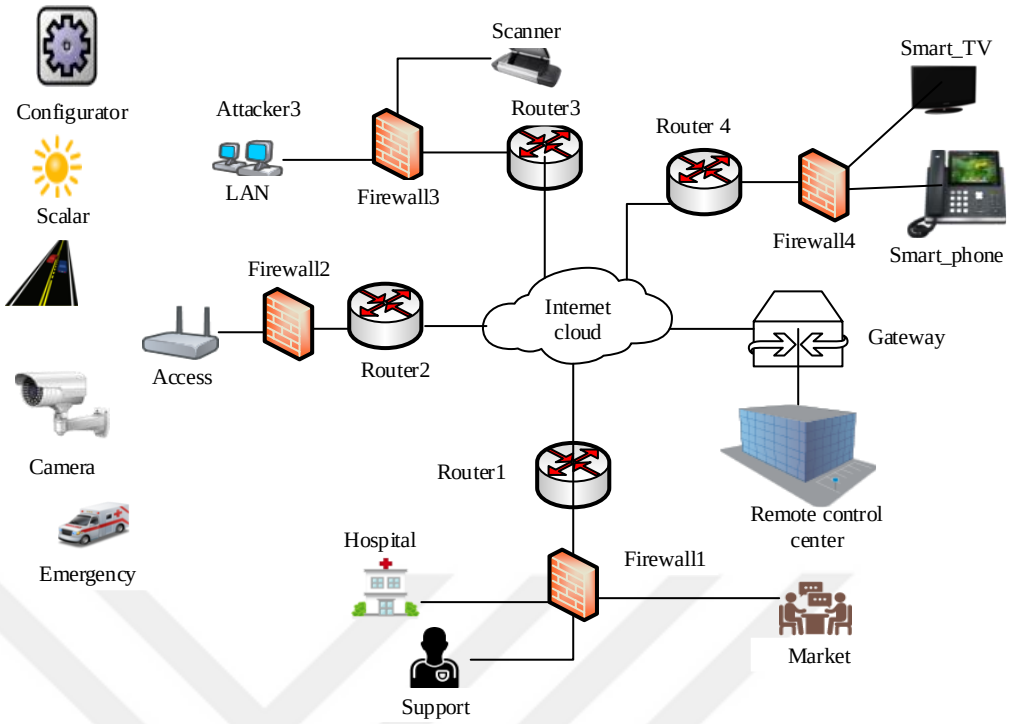

Figure 7.5. Simulated network without attack modules

7.4 Simulation Parameters

In OMNET++, the parameters are variable that apply to a module and can be used for building network topology (number of router, host, switch, etc.). These parameters enable the customization of simple module behavior and can be assigned in configuration file and network event description (NED) file. The parameter can take a numeric, string, Boolean values and/or XML [56]. Table 7.1 shows the parameters we used in our simulation defining a different scenario and also specifying the movement pattern of the network. These parameters are fixed which are constant for the whole simulation. In the simulation, the first parameters we defined are the network size and simulation time limit. Secondly, the evaluation of wired and wireless network with 15 devices. Thirdly, the UDP message length sent with order of 1000B and intervals of 100ms with a CPU time limit of 600s. Finally, the size of Wireless Playground which is 1004mx1004m. Moreover, the simulation network has a data rate of 15360b/s, queue frame capacity of 100, power of 2mW, thermal noise of -85bm, speed of 200m/s etc. There are many parameters the influence the simulation.

Table 7.1. Simulation parameters

Parameters	**Values**
Network size	1004X487
Simulation time limit	60min
Number of nodes wired and wireless	15
Message length	1000B
Sending interval	100ms
CPU time limit	600s
Simulation Start time	Uniform(0.1, 0.15)
Number of UDP application	1
Local port	5001 & 5002
Destination port	5001
Wireless Playground	1004mX1004m
Transmitted power	2mw
Receiver sensitivity	-85dm
Receiver threshold	4ds
Visualizer updates canvas interval	100ns
Speed	200m/s
Queue frame capacity	100

7.5 Connection Channel

Channels are essential modules in OMNEET++. Normally, channels `are` similar to simple module and are coded using C++ classes. OMNET++ provides different channels include ideal channel, delay channel, and data rate channel. Ideal channel enables all forward packets without delay and has no parameter. Delay channel has two parameters including delay parameter which describes message propagation delay and disabled parameter which is set by default to Boolean false and it drops all forwarded messages if the setting is true. Data rate channel has many parameters compared to delay channel. These parameters include double parameter that describes the rate of data transmission and bit error rate parameter which describes error rate. Moreover, the INET simulation model provides many network connection channels. For example, in Figure 7.4 and 7.5 network topologies, we used data rate channel and Ethernet Eth100M (is an Ethernet link of 100megabit/sec) channel [57]. The following subsection explains the module that we implement in our simulated networks.

7.5.1 Core of Network Module

The core of a network is an essential component of communication network, which enables primary node (devices) to connect to the network. It also routes the information between two or more sub-networks. The core of a network is facilitated with devices like router, switch, IADs and edge devices (for example, MAN, WAN), and has mesh topology

connection. In general, core of a network provides the following functions: aggregation, authentication, switching, charging, and also acts as a gateway between the networks. To simulate Internet core of a network, the INET simulation model provides a unique module known as Internet cloud. This module allows specific representation of network core and has distinct input parameters such as delay parameter which defines the time taking for sending a packet to the destination, drop parameter which defines the dropping packet probability, src parameter which gives the details about packet source, dest parameter which defines the packet destination, and data rate parameter which measures the rate at which date is forwarded from the source to destination (throughput link). Moreover, Internet cloud module enables the devices to have different probability drop and delay for clear input devices information, and it is stored in extensible markup language (XML) file [58]. For example, the below XML code, Internet cloud network is placed between the routers and gateway, the delay of these routers are calculated using normal distribution with standard deviation of 60ms and mean of 220ms. The data rate of the routers is between 100kbps and 1Mbps, and the probability of drop packet is between 0. 1 and 0.01.

```
<traffic src="sender [0]" dest="recipe" delay="20ms+truncnormal (200ms, 60ms)" datarate="uniform (100kbps, 1Mbps)" drop="uniform (0, 1) &lt; 0.01" />
```

As shown in Figure 7.6, Internet cloud compound module has five modules include: Internet cloud network layer module, interface table module, IPv4 routing table module, and Pcap recorder module, and wired network interface card module.

Firstly, Internet cloud network layer module is a compound module that includes: IPv4 which is a simple module describes IPv4 protocol (function as IP decapsulation and encapsulation, routing, assembly and fragmentation), ICMP simple module which handles Internet Control Message Protocol (ICMP) error packet and also enables the application of ICMP echo messages, Address Resolution Protocol (ARP) simple module which enables dynamic rendering of Internet Protocol (IP) addresses to media access control (MAC) addresses and error handling simple module which handles error notification messages [59]. Internet cloud network layer module has interface module known as cloud delayer. Cloud delayer is an interface module that drops/delays packets based on the arrival and departure to/from interface card packet. Cloud delayer interface has simple module known as matrix cloud delayer (this module delays and drops an incoming packet that is specified in XML configurator). IPv4 node configurator simple module is another type of Internet cloud

network layer module which acts as a link between the global network configuration module and the node. Secondly, interface table module which is a simple module that contains network interfaces table of the host. Thirdly, IPv4 routing table module which is a simple module contains IPv4 routing table. Fourthly, the Pcap recorder which is a simple module that records sent/received frame within devices (host). Finally, wired Network Interface Card (NIC) which is an interface that contains compound module like Ethernet interface compound module

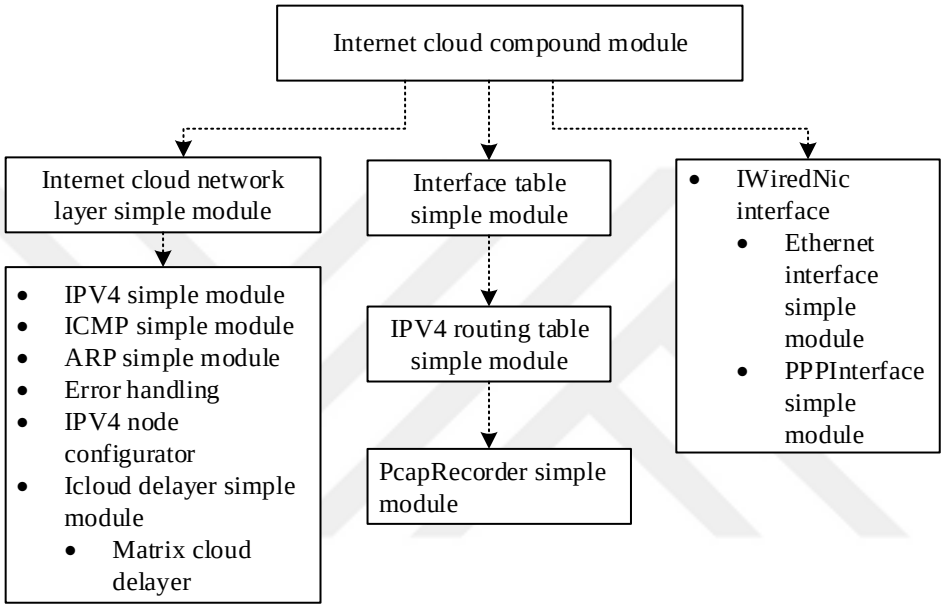

Figure 7.6. Internet cloud modules

7.5.2 Router Compound Module

A router is a network layer (OSI model) device that forwards and directs a data packet within a network. Router can connect two or more networks; for example, ISP, WAN, and LAN network. Moreover, a router acts as a gateway; the gateway is a device that enables the access to another network. To simulate a router, the INET simulation model provides a module known as router module. Router module is a compound module that enables the simulation of routers and supports network technologies like Ethernet, PPP, wireless and external interfaces. In the module, no any external interface, dynamic routing, and wireless are added by default. The router compound module can be connected to nodes via Ethernet gate and by default supports full duplex connection.

The design of router compound module is shown in Figure 7.7. The module consists six interfaces including: IP routing interface (IP routing interface is an interface for routing protocol module that is connected to Internet protocol layer and have OSPF routing simple

module), UDP Interface which supports UDP protocol and have UDP simple module, TCP interface (supports TCP protocol and has modules like TCP simple module and TCP spoof simple module), PIM routing interface which has PIM routing compound module, UDP application interface which supports UDP application for example DHCP client, DHCP server, etc., and BGP routing interface which supports routing of BGP module.

The router compound module has submodules include node status simple module which records the status of the node, energy storage interface module (this module defines the amount of energy produced by the generator and also the provided energy to devices and has a simple module known as energy storage base), energy generator interface module which outlines the process of energy generation, and mobility interface module which defines mobility models. In addition, router module has routing table interfaces include routing table interface (supports generic routing table, IPv4 routing table, IPv6 routing table, and multi-routing-table), table interface which tracks network interface table, and Pcap recorder simple module (this module traces sent and received frames).

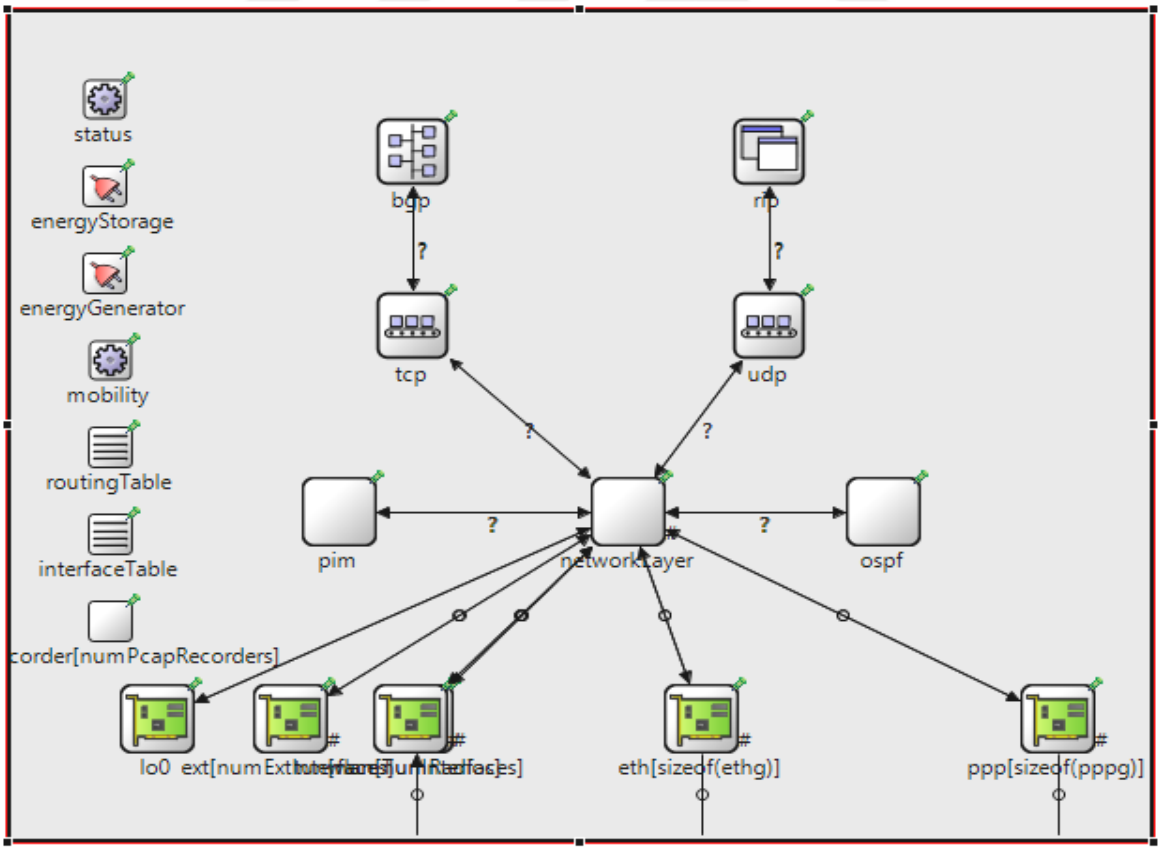

Figure 7.7. Router compound module

7.5.3 Access Point Compound Module

Access point is shortly known as WAP (Wireless Access Point). Access point is a wireless technology device that allows Wi-Fi (Wireless Fidelity) devices to connect to Ethernet wired network. Access point devices are mostly connected to wired router, hub and key which acts as a standalone device. It stores applications like software, security protocol, and firmware. Moreover, wireless access point device has three modes that are repeater mode, default mode, and bridge mode [60].

In simulation of wireless access point device, the INET simulation model provides a module known as access point module. The access point module is a compound module that enables the simulation of multiple wireless radios and multiple Ethernet port. Ethernet MAC, wireless card, and relay unit can be stated as parameters in the simulation.

In designation of the module, the access point compound have five interfaces and two simple modules: mobility interface (this interface supports mobility model), MAC relay unit interface (provides features of Ethernet switch), wireless NC interface, MAC address table, wired NIC, node status simple module and interface table simple module as shown in Figure 7.8.

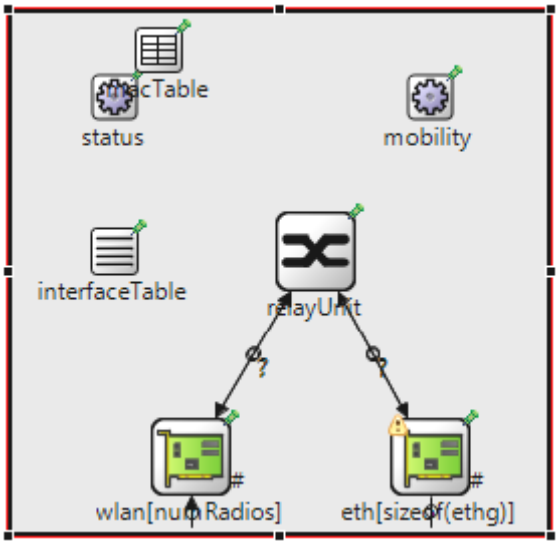

Figure 7.8. Access point compound module

7.5.4 Host Module

A host based on INET simulation model is any device that is connected to the network. It provides information, service, and application to the nodes (devices) that are on network. To simulate any device of wired and wireless network in OMNET++, INET model provides two compound modules known as Standard Host and wireless Host module. Standard host

module is a compound module of IPv4 host that supports TCP, UDP, SCTP and application layers. Standard host is mostly used in wired network and can be connected to another node via Ethernet interface (using Ethernet gate). By default, standard host module supports full duplex connection (only twisted pair is supported). In standard host module, no wireless card set by default, but can be configured using radio parameters. In addition, the external interface of the module can be configured using parameter and external interface module.

During designation of the module, the module consists of eight interfaces and one channel (ideal channel module). These interfaces include: Tun application interface module (this module has loopback application simple module), SCTP app interface module which has five simple modules (SCTP client, SCTP NAT peer, SCTP NAT server, SCTP peer and SCTP server simple modules), Ping application interface module, UDP Interface, TCP interface, TCP App interface, UDP application interface and SCTP interface module which support SCTP protocol.

As shown in Figure 7.9, the ad-hoc host module is a compound module of wireless network that has routing protocol, battery component, and mobility. ADHOC Host module supports IPv4 protocol, ICMP, and TCP/UDP transportation layer protocol. By default, it contains only one wireless card, but more can be added using radios parameter. It allows the implementation of wireless NIC and mobility interfaces.

In designation of the module, the module has many interfaces, for example, Manet routing interface module, TCP application interface module (This is a template for TCP application that specifies which gates TCP application needs and has simple module like HTTP browser, HTTP server, HTTP server evil and TCP generic server application, etc.), and UDP application interface module (this interface module supports TCP applications and also shows the gates that UDP application needs, and contains simple module like DHCP client, DHCP server, RIP routing, simple VoIP receiver and simple VoIP sender etc.), and ideal channel.

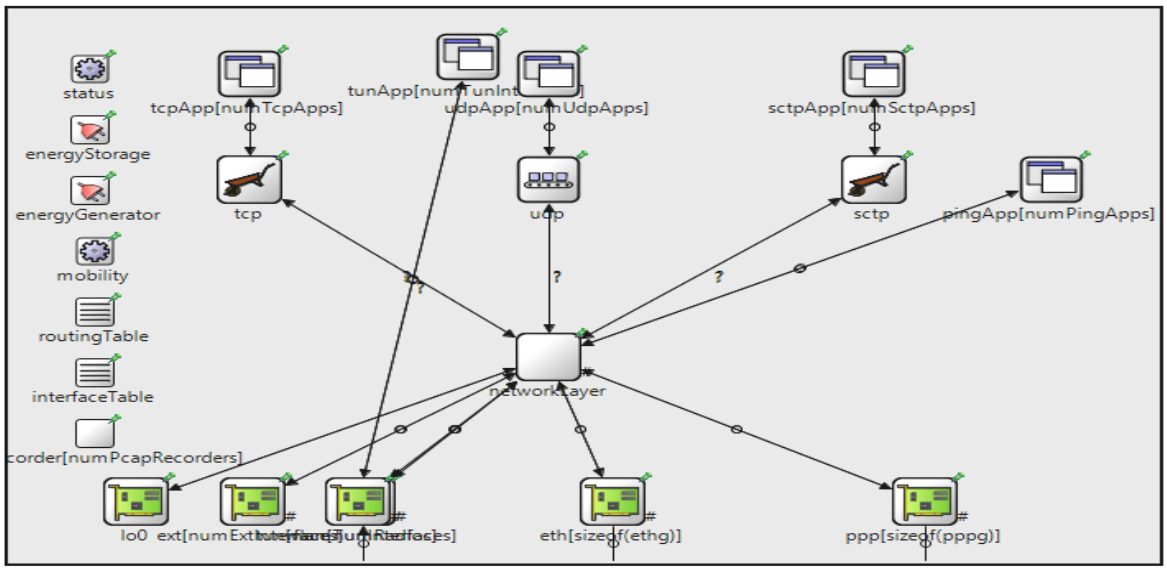

Figure 7.9. The ADHOC host module

7.5.5 IPv4 Configurator Module and IP Address Attribution

IPv4 network configurator module is simple module of INET simulation model. This module allows a network topology to have IP addresses and sets static routing. IPv4 configurator module, during assigning IP addresses, takes subnet into the account for each interface of the network. It enables optimization routing table. In IPV4 configurator module, the hierarchical routing is set using configuration fraction entering with a comparison of a total number of the nodes (devices). In addition, IPv4 configurator module supports both automatic and manual of IP assignment; for example, you can design a network topology with unspecified parts of IP addresses and netmask, and the configurator automatically puts the nodes addresses. By default, IPv4 configurator module adds routes, subnet based routing and can be turned on/off using NED parameters. The configurator use XML file to specify the network details (netmask, subnet, interface address, manual routing etc.).

The configuration of IPv4 module goes through a listed step: Firstly, building a network topology that has network node properties (these network properties include host, router, switch, layer two devices, access point, hub etc.), then assigning activities to the network. For internal use, the configurator creates a table to all connected nodes. The connected node sets network interfaces of the same LAN. Secondly, assigning IP addresses to all nodes and specifying the manual routes of the configuration. Thirdly, enabling static routing to all routing table of the networks and optimizing the routing table's size. Finally, results analyses.

7.5.6 IEEE 802.11 Scalar Module

IEEE 802.11 standard is used for WLAN network and it defines the MAC and physical layer. This standard is developed and maintained by IEEE. To simulate IEEE 802.11 standard, the INET model provides a module known as IEEE 802.11 scalar module as shown in Figure 7.10. IEEE 802.11 scalar module is a compound module of radio medium model that transmits energy in analog. The module is used with conjunction of IEEE 802.11 scalar radio model (a radio model that uses scalar transmission).

IEEE 802.11 scalar module consists of nine module interfaces include: Propagation interface (a module interface of propagation model that specifies propagation radio signal over time), path loss interface (describes power reduction when a signal propagates over a time), analog model interface (describes analog model, obstacle loss interface specified the obstacle loss model), radio background noise interface (describes the background noise model), medium visualizer interfaces (describes a simple module known as medium visualizer), medium limit cache interface, neighbor cache interfaces and communication cache interfaces (includes three compound modules namely map communication cache, reference communication cache, vector communication cache).

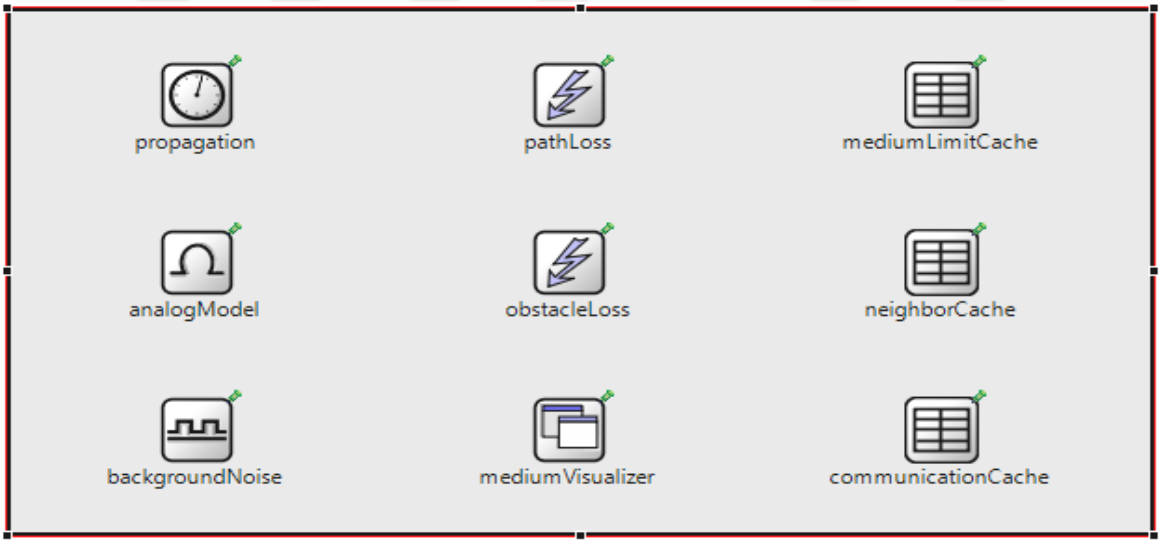

Figure 7.10. IEEE 802.11 scalar module

7.6 New Extension Module

7.6.1 Firewall Extension Module

The term firewall was originally referred to a wall that prevents the spread of fire and was used by firefighters. Before the emergence of firewall in 1980, computer network used

access control lists to secure the network. Access control lists are deployed on router which determined IP addresses and allows or denies access to the network. In networking, a firewall is an integrated collection of network security system that can be either hardware or software based. Firewall monitors network traffics, work based on specifies network security rules. It creates a trusted environment between interior and exterior of the network. Moreover, firewall consists of two categories that is host-based firewall and network firewall. The host-based firewall enables a host to have a layer in software which prevents the host from unauthorized access [61, 62]. Network firewalls are application software run on a hardware which filter two or more networks traffic. The firewall also acts as DHCP and VPN server for the network. As shown in Figure 7.11, when a packet is sent through, the firewall will have three conditions. Firstly, accepted, describes the packet that is allowed to pass through firewall. Secondly, dropped, specifies a packet that is not allowed to pass through firewall and no indication failure. Finally, rejected, describes that the packet is malicious.

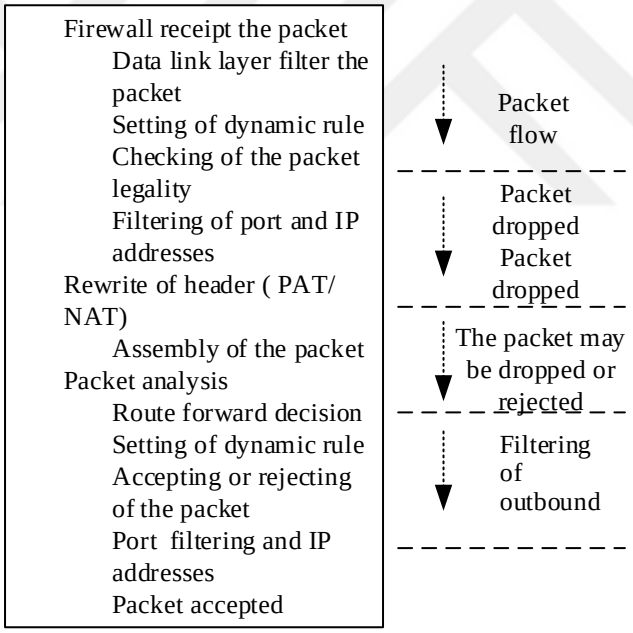

Figure 7.11. Firewall data flow and operation

In simulating a firewall, INET simulation model does not provide any module that will support the simulation of firewall. We designed a new extension module in OMNET++. This new extension module enables the simulation of different types of firewall. During the design of the module, we divided the module into three parts: accepted, rejected and dropped. This new extension module prevents malicious behaviors by accepting or blocking the network traffic and can restrain any traffic based on the port, IP addresses and

communication protocol (e.g. UDP, TCP etc.). However, this new extension module sometimes is unable to differentiate between malicious traffic and reliable traffic.

7.6.2 Attacker Extension Module

The network attack is a security threat to wired and wireless network. Therefore, attackers can forward a compromised packet to conduct various types of network attacks. This forgery packet prevents legitimate users and keep the network busy by consuming the network resources. The target devices is flooded with TCP/UDP packet.

In attacker module, we developed new extension module for OMNET++ as shown in Figure 7.12. We applied this new extension module to OMNET++ to enable the simulation of different types of network attacks. This new extension module has three different types of attacks. Firstly, drop attack; this is a type of DDoS attack whereby an attacker consumes the network resources and is usually occur on the router. Secondly, delay attack; this is a man in the middle attack whereby an attacker delays the time synchronization of sending packet between devices and mostly occur on sensor networks. Thirdly, sinkhole attacks; this type of attack enables the attackers to establish a connection and have root access to create backdoor in target system. Moreover, this new extension module enables us to define attacker's behavior and evaluate their effect on the network.

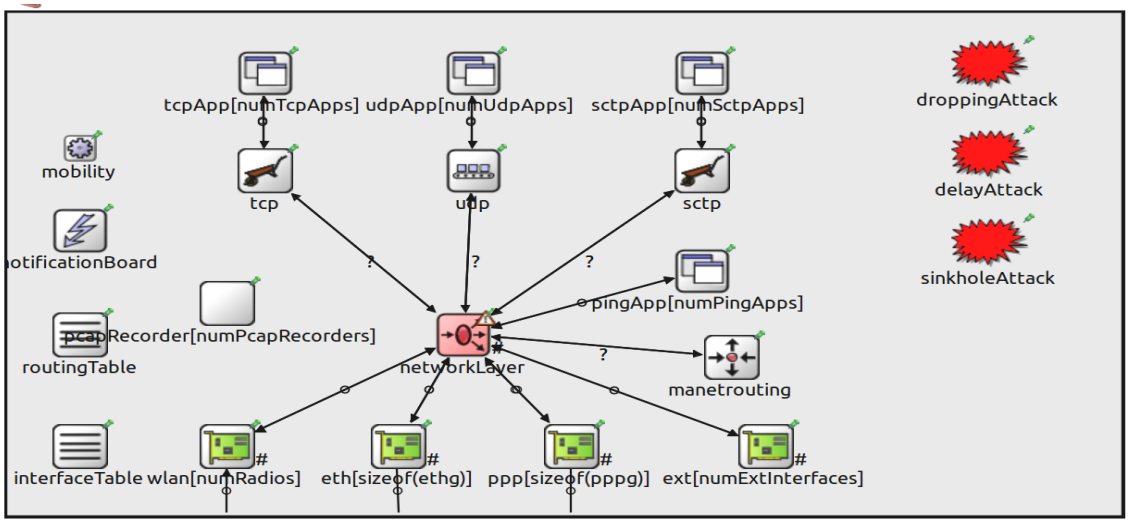

Figure 7.12. Attack module

In the design, attacker extension module is a compound module of IPv4 host and have UDP, TCP, SCTP and application layer. The module consists of many interfaces; for example, TCP and UDP application interface which describes the gates. This application interface has a module like HTTP browser simple module that enables the simulation of

browser on host, HTTP server simple module which describes how to simulate web, TCP echo simple module (this module defines how TCP accepting incoming connection using echo), and UDP basic burst simple module which describes how UDP sends packets to specified addresses in bust.

The attacker extension module has three essential modules that enable the attacker to launch attacks including drop attack, sinkhole attack, and delay attack using simple modules. In the design of these three simple modules, we defined some attack components include messages controller, attacks module and hacked module. Messages controller enables messages between attackers and modules. It also has that necessary information for attacks execution. Moreover, messages controller also enables the activation/deactivation of different types of attacks. As illustrated in Figure 7.13, hacked module is a compound and simple module that enables attack strikes. Attack module is a simple module that controls attack execution and contains three important properties as shown in Table 7.2.

Table 7.2. Attacks module properties

Attacks module properties	**Description**
Attack type	This is a name that distinguishes attack types
Start time	Defines the attack simulation start time
End time	Defines the attack simulation end time
Attack parameters	Defines parameters dependencies
Active	This is a Boolean statement that enables the activation and deactivation

We briefly explain the attack implementation based on attacks behavior and parameters. Firstly, drop attack module that drops a packet deliberately using probability. This module also accepts packet instead of sending and interrupting network services. Moreover, the essential parameter of drop attack is dropping attack probability (this drop attack probability parameter describes the probability of a packet dropping and it is set to 0 by default). Secondly, delay attack module that describe how a malicious node can delay a packet, and it has an attack probability parameter and delay attack value parameter (the attack value parameter defines time delay used for each packet). Thirdly, sinkhole attack module that enables compromised node to send a malicious routing information, and has parameters like attack probability and number hops, etc.

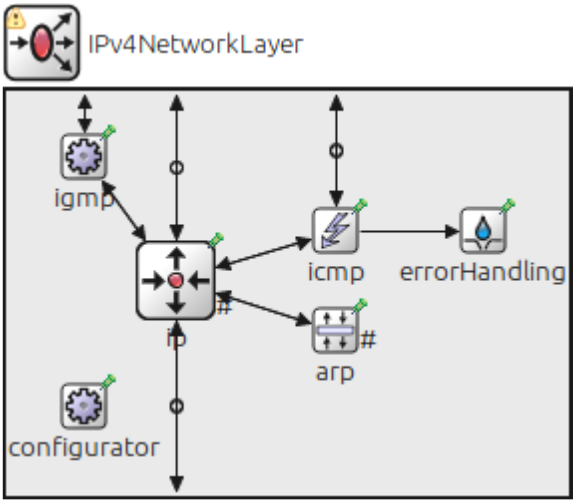

Figure 7.13. IPv4 network layer compound module

8. PERFORMANCE ANALYSIS OF THE APPLICATIONS

OMNET++ IDE provides tools for simulation results analysis and visualization. These tools enable the user to load distinct files, results browse, and data selection. It allows users to plot various charts and graphs using scalars and vector data. Moreover, the OMNET++ IDE enables step processing, various charts and graphs creation, and a combination of both for efficient results [63]. As shown in Figures 7.4 and 7.5, we simulated a network topology with maximum number of devices, sources, destination, services provided and time limit of 60min. Therefore, the simulated network has a link between devices which enables communication, packets transmission and routes a packet to a remote center where decision and analysis are taking place.

To obtain various results of our simulation, we focus on several aspects including: throughput which measures the rate of data transfer from source to destination, end to end delay which describes the time taken for a packet to arrive its destination, energy consumption which defines the amount of power consumption by the system, packet loss ratio, packet queue which describes sequential order of a packet, attack evaluation and error rate which measure the rate of corrupted packet. Moreover, for each performance analysis, we evaluated the effect of various types of network attacks on M2M communication and we compared the result with network topology that has no any attack implemented attack module (as shown in Figure 7.5). The evaluated results can be viewed in the form of tables and graphs. In order to understand network security problem for M2M communication, in this chapter, we present the results performance related to previously simulated network topology (Figure 7.4 and 7.5).

8.1 Performance Analysis of Network without Attack Module

8.1.1 Network Throughput

The emergence of networks large-scale users such as M2M communication increases network complexity. These network complexities are now considered as current existing network problem due to simultaneously sent huge amount of packets on a network. The network provider uses throughput to analyze some of these network problems. The Network throughput is the process of measuring the rate of successful delivery messages from source to destination and the messages are delivered over logical link. Network throughput is generally measured in bits per second, data packets per second and data packets per time slot. Network through also known as bandwidth digital consumption, which sums the rate of

delivering data in a network using queuing theory (queuing theory is the process of using mathematical studies to deliver data in a waiting line). Throughput sometimes affects various network communication systems including physical analog medium, power component, and end to end users.

The network throughput can be computed as follows:

$$\text{Throughput} \leq \frac{\text{RWIN}}{\text{RTT}} \quad \textbf{(8.1)}$$

Where RRT describes round trip time and RWIN describes TCP receive window size [64,65]. For example, assume a network has TCP window size of 65,535 bytes and trip time of 0.220 second, to compute the maximum throughput just divide amount of successful delivery data with time taken to arrive destination. When we divide 65,535bytes/0.220second the maximum throughput is 2.383 Mbit/s.

In our simulation, the INET framework provides many compound modules that enable the simulation of network throughput include throughput client module, throughput sink module, and throughput server module.

A throughput client module is a compound module that has circled mobility simple module (this module enables a node to move within a circle). Throughput server module is also a compound module which consists of stationary mobility simple modules that describe the stationary nodes, sink simple module, and IEEE 80211 NIC compound module which enables IEEE 802.11 network interface card implementation.

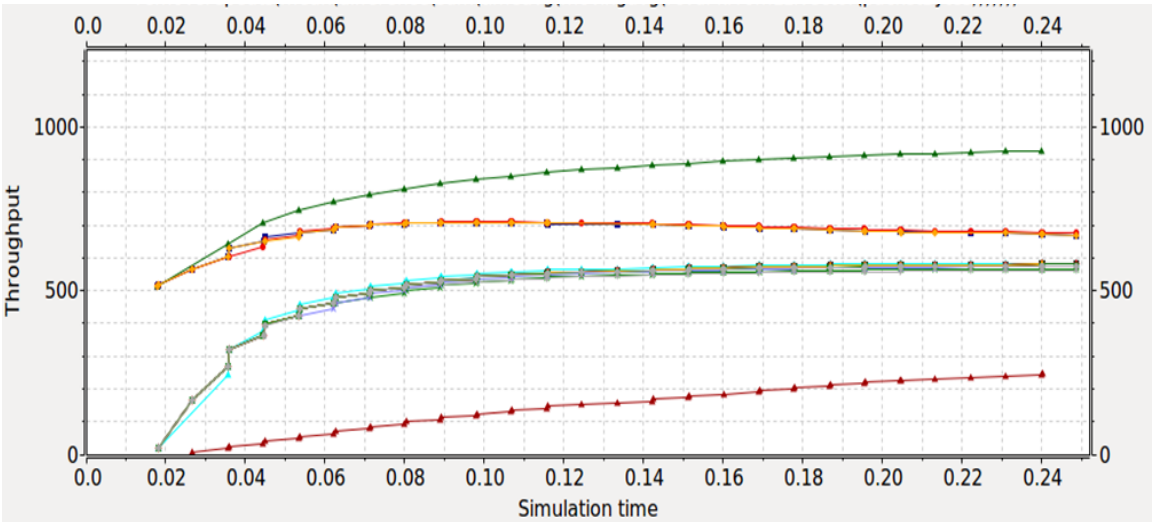

Figure 8.1. Network throughput

The network throughput is an essential metric for evaluating M2M network performance and the capacity of successfully delivered ratio. As illustrated in Figure 8.1, the messages belong to network throughput of our simulated network topology (Figure 7.5) whereby data is delivered over logical link to destination using previous simulated network topology. In the graph, the x-axis represents the time taking to arrive to destination measured in seconds while the y-axis describes the throughput. These messages are sent over UDP protocol and have constant data rate, we analyze the process, and the result showed that maximum throughput is approximately 900.1 bits/sec. The reason for packet drop is due to the network involvement of higher delay rate whereby a huge number of M2M devices try to access the network at the same time, leading the devices to collide and this causes most the devices to wait before accessing the network for certain amount of time.

8.1.2 Energy Consumption

Nowadays, energy is a major parameter for designing networks equipment when we compare it with previous traditional network. It has drawn attention of many industries like wired and wireless communication centers. The energy consumption of IT industry like economic cooperation organization, it has been estimated about 2 percent of total energy, and transmission, switching, access network approximately consume 0.5 percent. In M2M communication network, optimizing energy consumption is a major concern. This energy is mostly consumed by network access devices. These network access devices include Internet Protocol, satellite, UTRAN, etc. and they enable the communication between M2M devices and network core. They are primary factors that network providers need to focus on.

To simulate the amount of consumed energy, the INET simulation model provides a modules that enables the simulation of energy consumption. These modules include: Firstly, energy consumer interface module which is a compound module that defines consumed amounts of energy by devices and the time taken to consume the energy. For example, devices like satellite and radio consume energy when receiving, transmitting and processing a signal. Moreover, these devices consume a lot of energy when turning on. Energy consumer interface module has a simple a module known as an energy consumer base module which enables signal sharing and statistics. Secondly, energy generator interface module which is an interface module that describes the process of generating energy over time. For example, solar system panels are deployed toward the sun and weather conditions to generate energy over time. Thirdly, energy source interface module which is an interface

module that provides power to various consumers. The energy source module has two simple modules that is energy source base simple module and energy storage base simple module. Fourthly, energy sink interface module which is an interface module that absorbs power from multiple sink power generators and has a simple module like energy sink base simple module that describes network signals and statistics. Lastly, energy storage interface module that defines devices that consume energy. For example, mobile phone battery provides energy for functionalities like CPU, display, wireless devices and it consumes energy when it is plugged to charge [66]. Table 8.1 summarizes power parameters that we used in our simulation.

Table 8.1. Power parameters

Parameters	**Values**
Thermal noise	-85dBm
Energy consumption in Transmission	2mW
Energy consumption in receiving and channel sensing	135mW
Energy consumption in idle	1mW

In order to obtain a reasonable performance, we used previous defined modules. These modules enable us to evaluate energy consumption of both wired and wireless networks. Moreover, during the evaluation of energy consumption we took the whole network into account when devices send packets to the destination. Figure 8.2 presents the energy consumption of our simulated network. In the graph, we can see that as the number of nodes increases, the amount of energy consumed by sending one packet to destination also increases. The reason for this increment is obviously due to congestion and collision growth in the network. The graphs also reveal that energy efficiency of sending huge amount of packets is higher than energy efficiency of sending small amount packets.

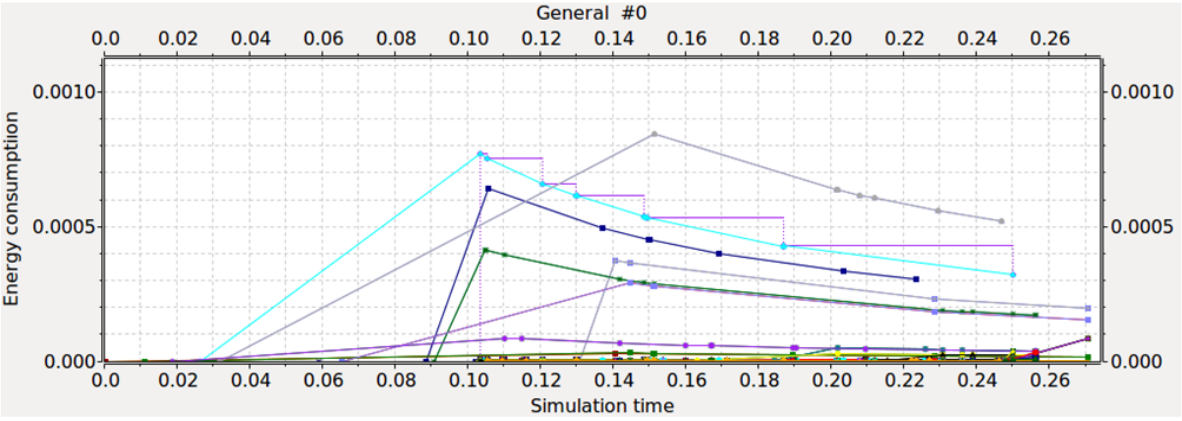

Figure 8.2. Energy consumption of sending packet to destination

8.1.3 End-To-End Delay

End-to-end delay is an essential component for evaluating network performance. There are various M2M applications that are sensitive to delay like VoIP, audio streaming and gaming. End-to-end delay refers to the time taken by data to be delivered from a source device to a destination across the network. End-to-end delay is also known as one-way delay which defines network IP monitoring. End-to-end delay metrics consist of four types, namely processing delay, queuing delay, propagation delay, and transmission delay. Processing delay defines the time taken by a node to process a packet, and it also checks error bit, output link, and packet header. Queuing delay describes the time taken by a packet waiting in a queue for another to be transmitted. Queuing delay also determines output link transmission waiting time and congestion. Transmission delay defines the time required by the network to put the whole packet into communication media while propagation delay is the time taken by a signal to propagate from one node to another.

End-to-end delay can be calculated as follows:

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop} \quad \textbf{(8.2)}$$

End-to-end delay is measured in seconds. Equation 8.2 formula describes the delay of a packet when it routes from source to destination. The dproc stands for delay processing and is measured in bit/s, dqueue stands for queue delay, dtrans stands for transmission delay and can be calculated using L/R where L is the length of the packet in bit while R is transmission rate. dprop defines propagation delay and can be calculated using D/S where D is the distance taken from one node to another while S is the speed of the media [67,68]. For example, assume we are sending a file of 30Mbit of MP3 with transmission rate of 10 Mbps and length of 10,000 km, the file has a propagation speed of 2 * 108 meters/sec, the result shows that the network has end-to-end delays of 3.05second.

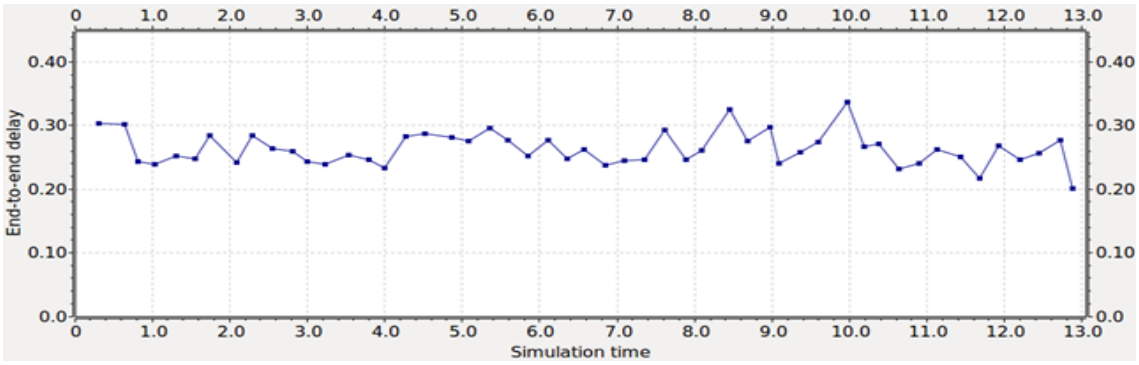

Figure 8.3. End-to-end delay

In our simulations, we deployed various numbers of devices and created a connection between them. We used UDP traffic while communication, then we computed the end-to-end delay by taking the time difference between the packet formations and time taken to deliver the packet to destination. Figure 8.3 presents end-to-end delay of our simulated network topology. From Figure 8.3, it is shown that as the number of devices increase the delay also increases. It is also revealed that when a larger packet is sent, the delay also increases.

8.1.4 Queue Description

In general, queue can be defined as a sequence of a work that is waiting to be handled. Queue normally uses first-in-first-out (FIFO) principle. As illustrated in Figure 8.4, in queue two activities are allowed enqueue and dequeue. enqueue is the process of adding activities into the queue while dequeue is the process of removing front activities. Moreover, queue provides essential services to research center, computer sciences and transportation where distinct items such as event and data are added and to be processed in a sequential order. Queue does not usually have specific limit. Therefore, new items can be added consistently and regardless of how many items are already contained.

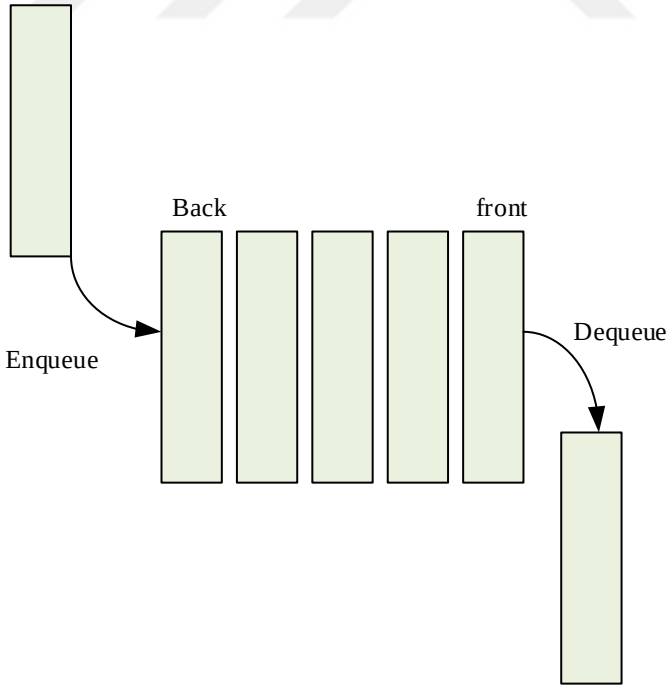

Figure 8.4. Queues activities

In the simulation, the INET simulation model provides various queue modules including: The drop tail queue module which is a simple module that can be used inbuilt network

interfaces. Drop tail queue module can also be used as a key component of output queue interface module. FIFO Queue module which enables the implementation of FIFO queue and can be associated with schedulers and drop algorithm to form output interface module. The ether QoS queue module which is a compound module that defines pause frames as a first concern. Red queue module which is a compound module that contains FIFO queue and red dropper module, and can be used in measuring network performance. In our previous simulated network topology (Figure 7.5), we used drop tail queue module.

Figure 8.5 and 8.6 show the simulation result of queue time (queue time is the amount of time taken by activities before being handled.) and queue length (queue length can be defined as set activities of an individual). In the graphs, we can see that all the packets are sent in a queue. The figures reveal that the packet is sent based on FIFO principle and the storage capacity is limited. The figures also show that the queue accepts any new packet until it's full, then it drops the packets. When comparing the simulation results of Figure 8.5 and 8.6, it is clear that the result complies with queue theory.

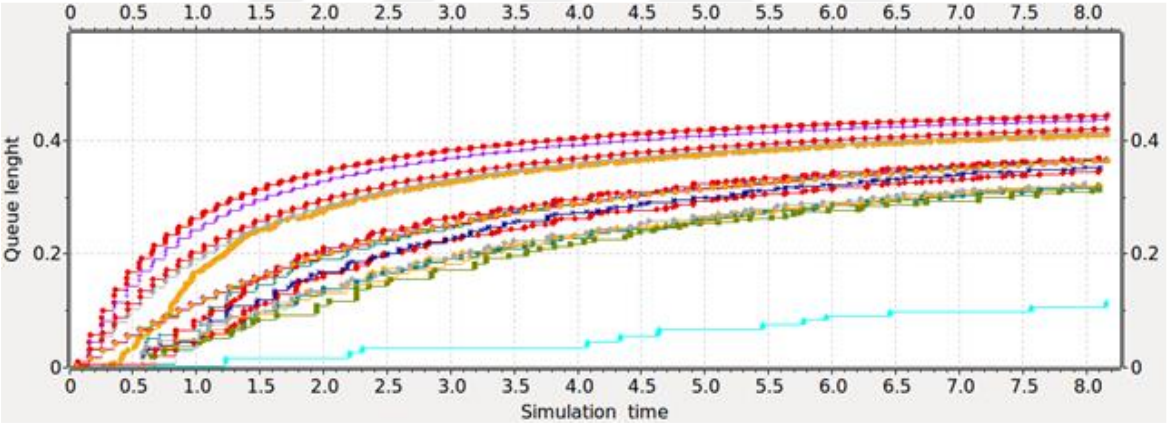

Figure 8.5. Queue length

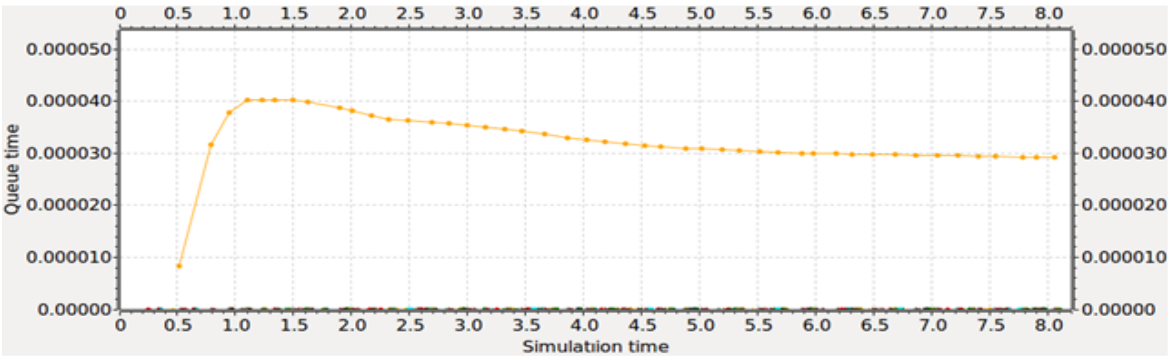

Figure 8.6. Queue time

8.1.5 Sent and Received Packet

The objective of network simulation is to gather an information, data, and event from the simulated network for visualization. In our simulation, we gathered information on sent and received packets to show the inefficiency, a particular pattern, breaking point of M2M communication network. Sent packets describe the amount of packets sent by devices while received packets is the amount of packets that devices receive. For example, in Figure 8.7, we can see that the packet received through input and output gates. If a device does not receive the packet, then network will update the received signal again. Moreover, in our simulation, the packets are sent over UDP protocol where receiving devices acknowledge the packet and it possible to send a packet before acknowledgement.

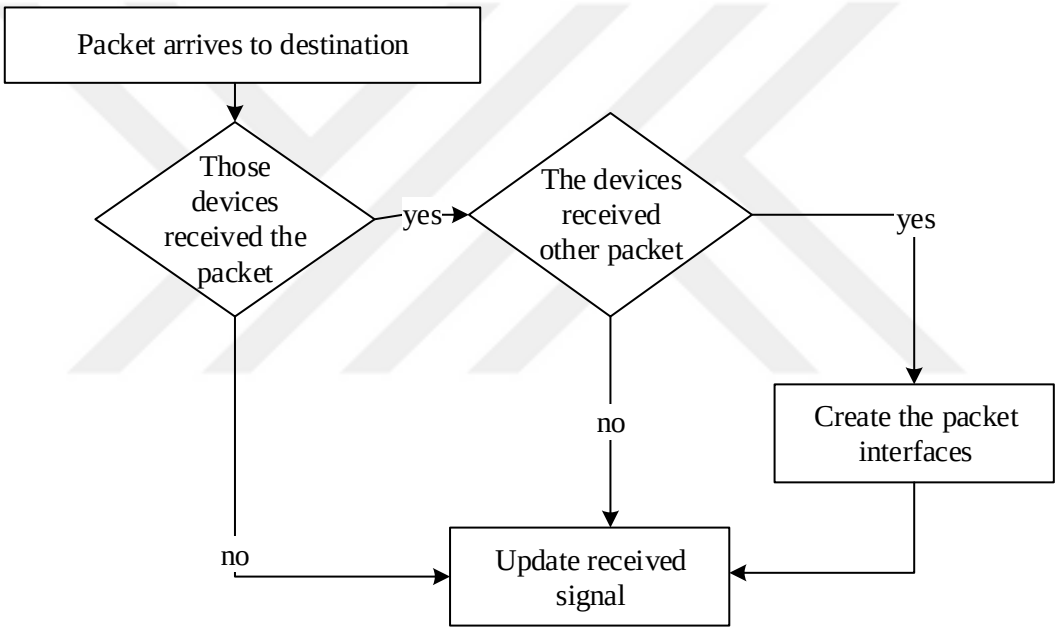

Figure 8.7. Queue time scheme

Figure 8.8 shows the amount packet sent over wired and wireless network and how it changes over time. In the graph, we can see that each mark represents a sending packet and they rise a significant percent. Obviously, sending packet count is great when not any attacker's type is implemented. When attacker's type is added, the number of sending packets is fully affected. Figure 8.9 illustrates the result regarding received packets where some of the packets experience delay. Generally, when we compare Figure 8.8 and 8.9 some of the packets are dropped.

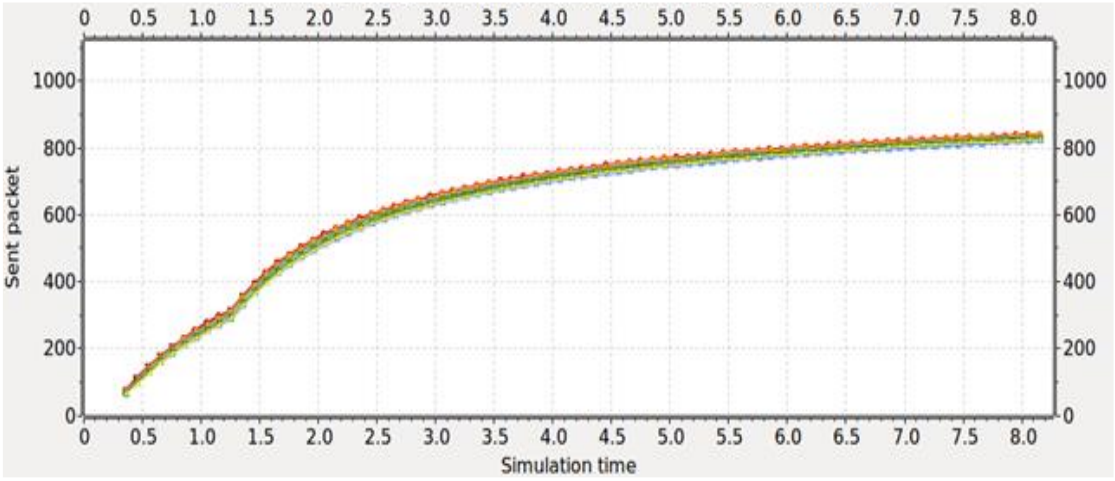

Figure 8.8. Sent packet

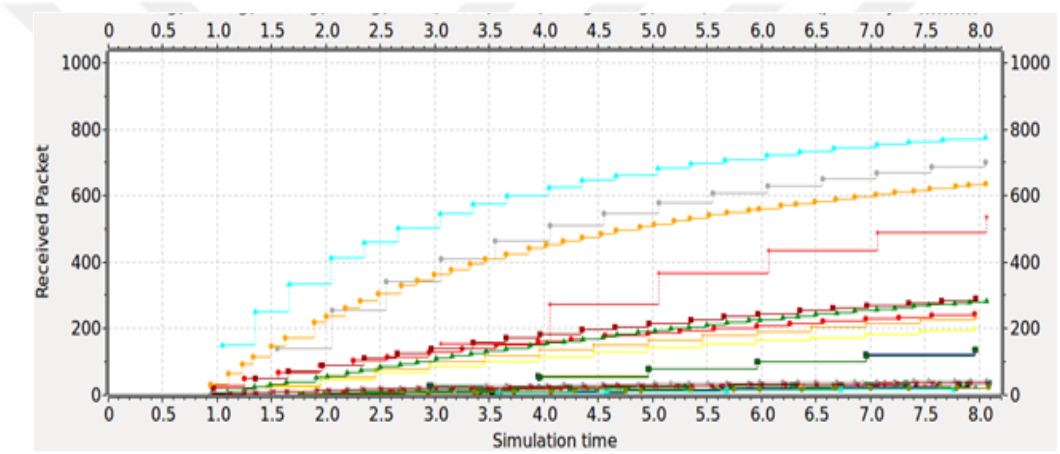

Figure 8.9. Received packet

8.2 Performance Analysis of Network with Attack Module

In attack evaluation, we simulated Figure 7.4 network topology and calculated many metrics including: sent packet, received packet, sinkhole attacks, end-to-end delay based on quality of service (QoS). To obtain accurate results, we also focused on UDP packet drop interruption due to attacks modules, packet drop ratio due to attack modules and UDP (user datagram protocol) quality of service also due attacks modules. Moreover, for each plot we investigated receivers, senders, and access points, and how distinct devices response to an attack. These metrics are discus as follows:

8.2.1 Attack Sent Packet

Sent packet describes the amount of packet sent in order to reach destination. Generally, attack modules lead to network congestion (network congestion describes the process whereby a network node forwards too many packets, which reduces the quality of network

service), loss of packet, delay, router failures (limited router packet queue cause packet drop) and reduce network throughput. Moreover, during sending packets, the attacks try to drop a packet with a specific probability and compromise the network services. It changes the existing network service transmission to slow, consumes more power resources, and increases the time intervals.

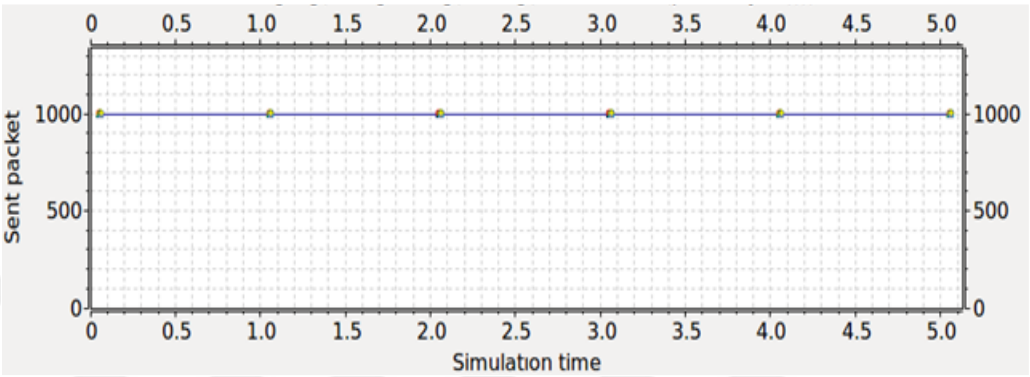

Figure 8.10. Sent Packet for attack network

In our simulation, we deployed distinct devices (nodes) and attacker's node (the attacker node forgery is a packet sent to target devices which causes packet delay based on certain probabilities). We transmitted 1000B of UDP packet from source node to remote center and destination. The simulation runs several times in an interval of 0.5 seconds.

As illustrated in Figure 8.10, we plotted a graph with vector recorded data. *x*-axis represents simulation time while *y*-axis shows the sent packets. In the graph, the attack starts at 0.1 seconds and then increases to about 5 seconds. Analyzing the results show that it is related to attack modules and also show that attackers can easily drop a packet and can easily take control of the network.

8.2.2 Attack Received Packet

In order to understand the effect of attack module on wired and wireless network. We analyzed received packet of the network. It is a total number of sent packet (this occur because of attack module) minus total number of received packet. In the simulation, we deployed devices with playground area of 1004m x 1004m square, these devices send a UDP packet of size of 1000B from sources to destinations. The simulation time set to 60min and runs several times.

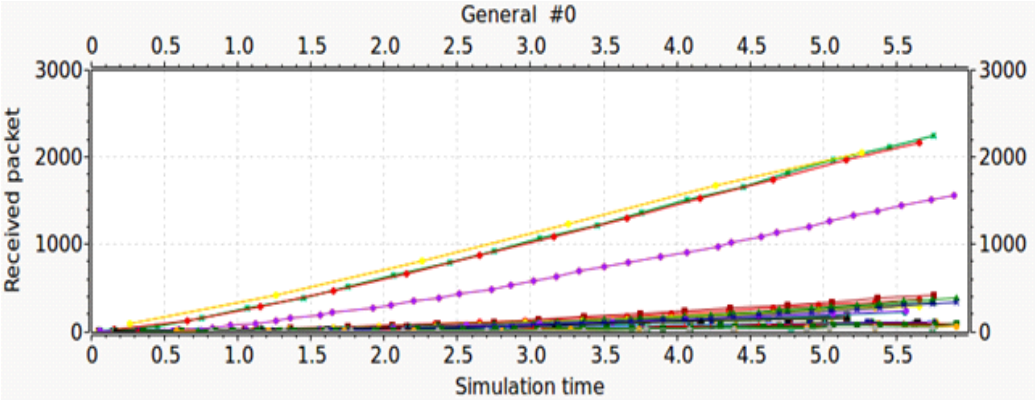

Figure 8.11. Received Packet for attack network

In figure 8.11, we plotted a graph of packet loss ratio whereby the *x*-axis represents the simulation time while the *y*-axis shows received packets. In the graph, we computed packet loss ratio between source node to remote center and destination. Attack modules are active for the whole simulation. The result shows that increasing the number of attacks slow the network performance, increase error rate and services. Moreover, increasing the number of packets results in collision, packet loss and error rate.

8.2.3 Sinkhole Attacks Evaluation

Sinkhole attack is the process whereby an attacker manipulates the network by creating fake nodes. In sinkhole, when the attacker rouges the network, this enables the launching of other attacks like ICMP attack, IP spoofing, selective forwarding attacks, etc. Sinkhole attacks also compromise routing information. In order to simulate sinkhole attack, we created a sinkhole module (the sinkhole module is a simple module that enables us to launch sinkhole attacks and various types of attacks) as explain in the previous chapter. To analyze the performance of sinkhole attacks, we plotted a graph using recorded data as shown in Figure 8.12. We defined a metric known as attraction ratio, which defines the total number of a packets that sinkhole devices (nodes) received to the total number of packets that are normally received.

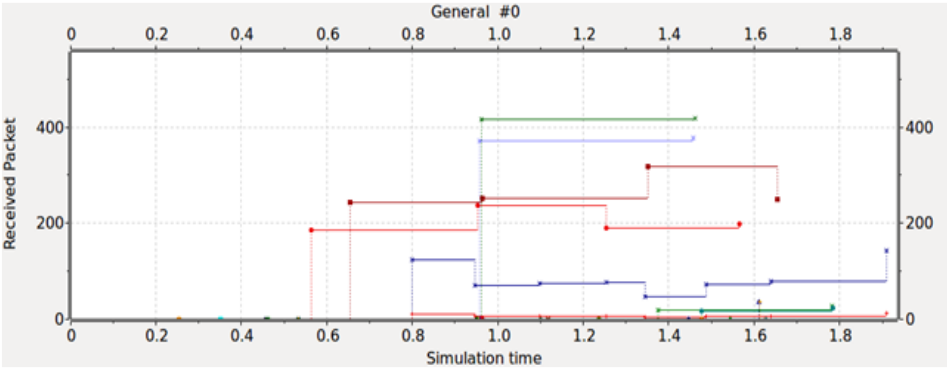

Figure 8.12. Sinkhole attacks evaluation

Figure 8.12 shows that sinkhole devices consume more nodes than legitimate nodes. The result also shows that when attack nodes increase, the attraction ratio decrease. Moreover, the number of attackers increase when total number of sinkhole attracts packet increase.

8.2.4 Quality of Services

M2M communication system is totally different compared to normal network communication. M2M communication uses huge amount of data for communication and no human intervention. In this scheme, we analyzed Figure 7.4 network quality of service. The quality of services (QoS) can be defined as the overall set of network performance and is governed by three parameters that is latency which describes end-to-end delay, bandwidth, and reliability. In order to secure M2M communication network, quality of services (QoS) is necessary for control monitoring such as bit rate, throughput, error rate, availability, and delay.

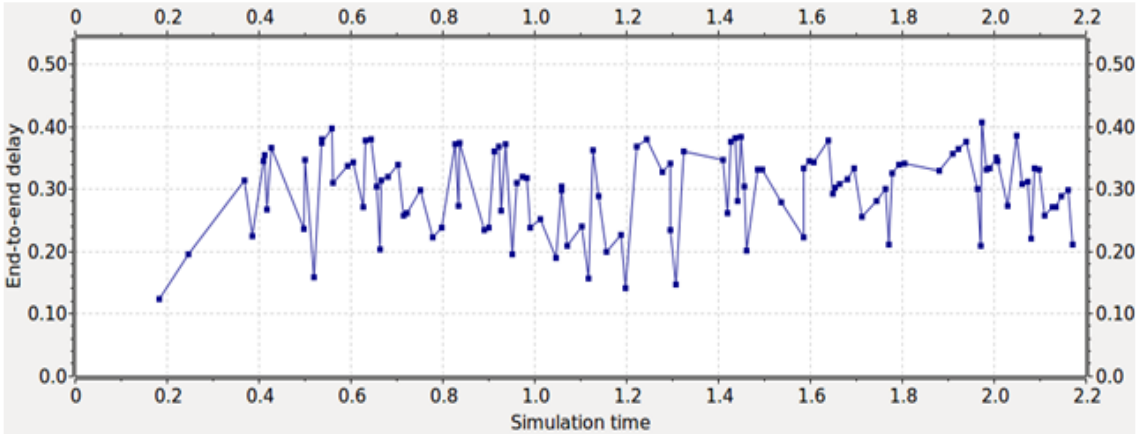

Figure 8.13. End- to-end delay of attacks networks topology

In Figure 8.13, we collected a vector data and a plotted end-to-end delay graph based on quality of services (QoS). In the graph, *x*-axis represents the time taken for network to send

a packet while the *y*-axis represents end-to-end delay. The figure reveals that network load and delay attacks modules do strongly affect the network performance. Therefore, as the network traffic increases, the error rate also increases, especially when the network is under attack. In addition, we observed that before the simulation goes under attack, the simulation time is 0.02 second. During the attacks huge amount of UDP packets transmitted. Some of the transmitted packets enter-queue while some are dropped. The packets that entered the queue had waited for a long time until the attack module finished processing, resulting in an excessive delay.

8.3 Comparison of Simulated Network Results

In this subsection, we compare network topology without attacks module and network topology with attack modules (Figure 7.4 and 7.5). In network topology without attack modules, we collected huge amount of data and analyzed the network throughput, energy consumption, end-to-end delay, queue description and sent and received packets while in network topology with attack modules, we analyzed packet drop, packet lost ratio, sinkhole attacks and quality of services (QoS). In order to have a significant comparison, we used the same packet size, UDP traffic, and the same simulation time. However, the comparison between these two topologies reveals essential facts shown in Table 8.2.

As shown in Table 8.2, we compared results of Figure 7.4 and 7.5 simulated network topologies. In Figure 7.5, the network throughput and packet loss ratio are low and caused by packet collision; while Figure 7.4 simulates the network topology the result shows huge packet compromise due to attack modules and packets dropped. When we compare energy consumption of Figure 7.4 and 7.5 networks, the result shows that Figure 7.5 network consumes more power compared to Figure 7.4 network because of the attack modules. In terms of queues, we observed that Figure 7.5 network starts processing normally then it changes over time due to the collision while in Figure 7.4 network has a queuing problem because the node sent huge amount of traffic and attack modules try to manipulate the network. In addition, in Figure 7.5 network, sent/received packets is due successfully compared to Figure 7.4 network because the traffic only send/receive by legitimate nodes. And in both networks when number of nodes increases, it results in high collision, delay, increase in time and consume more power, etc.

Table 8.2. Comparison of simulated network result

Statistic Module	Network topology without attack module	Network topology with attack module
Network throughput	In this network, we analyzed network throughput and plot a graph shown in Figure 8.1, the result shows that the network has intermediate throughput.	In this network, we measured the throughput based on quality of services and the result shows that more packet was compromised.
Energy consumption	This network shows low energy consumption.	The simulation results show that this network consumes more energy and results in service denial, packet drop and delay
End-to-end Delay	End-to-end delay is low compared to Figure 8.13 network and also has low simulation.	The network has a high end-to-end delay time which increases in each simulation because of attack modules
Queue description	In this network, packets delivery are based on queue and the Figure shows that sometimes there is a collision in the network.	In this network, most of the packets are dropped from the queue.
Sent and received packet	Collision happens when more than one devices try to send/receive a packet at the same time.	Throughout simulation, attackers are able to send and receive packet.
Sinkhole attacks	No attack modules.	In this network, sinkhole attacks rouge the network and result in more damage such service delay and packet drop.
Quality of services (QoS)	In this network, we simulated quality of service and we analyzed end-to-end delay, throughput, and energy consumption.	We analyzed Quality of services (QoS) based on an end-to-end delay and the result that the network has an end-to-end delay because of the attack module.

9. CONCLUSION

After giving a detailed explanation, this thesis concludes that the M2M communication is a set of automated connected devices that remotely allow wire-line and wireless to exchange any information without human intervention. It transfers data on device and physical asset to central remote station for sufficient control and monitoring. While the M2M communication concept has been in use for a quite long time, but the growth of business case acts as a newer motive that stimulates its growth. The M2M communications can be used in design strategies for many applications such as smart grid, manufacturing, healthcare, utilities, and security, etc.

In this thesis, firstly we provided a good understanding of M2M communication based on its architecture, characteristic, standardization and how it works. Secondly, we explained the related work, M2M communication technologies and for effective communication and secure connection of M2M communication network, we also discussed M2M network security challenges and threats which include jamming attack, hello flood attack, sinkhole attacks, and configuration attack, physical attack, DDoS and falsification attacks. Thirdly, we explained common existing solution of network security problems. These solutions include 3GPP/4GPP, key management, intrusion detection, replay protection, IP security, COAP security and IEE 802.15.4 security.

In M2M communications, recent studies have been presented in developing of M2M network standard, but these standards do not provide a good solution that will support M2M communication in terms of minimizing energy efficiency, scalability, reliability, security, and diversity of Quality of Service (QoS). In this thesis, we presented a comprehensive simulation for M2M communication network security problems such as performance and threats. To obtain accurate results of different parameter, we used OMNET++ simulator and INET simulation model. Furthermore, we also discussed the movement of packets from source to destination, new attacks extension modules which enabled us to implement many different types of network attacks and we compared two network topologies. In the simulation, we were able to simulate the network and obtain many useful results. We used the output results to plot various graphs including network throughput, energy consumption, end-to-end delay, sent and received packet, and quality of services (QoS). The result shows that there is a substantial reduction in network problem when UDP traffic is considered in network topology without attack modules when compared to network with attack modules.

In network with attack modules, the result proves that attack modules exploit the M2M network and degrade its performance and increase end-to-end delay, packet loss and power consumption.

REFERENCES

[1] **Li, X., Cai, J. and Zhang, H.,** 2013. Topology control for heterogeneous connectivity requirements to sink in m2m networks, *Communications and Networking in China (CHINACOM), 8th International ICST Conference*, Guilin, 1-10.

[2] **Dhraief, A., Belghith, A., Drira, K., Bouali, T., and Ghorbal, M. A.,** 2013. Autonomic management of the HIP-based M2M overlay network, *The 4th International conference on ambient systems, networks and technologies (ANT 2013), The 3rd International Conference on Sustainable Energy Information Technology (SEIT-2013)*, Halifax, Nova Scotia, Canada, 1-8.

[3] **Xie, M., Han, S., Tian, B. and Parvin, S.,** 2011**.** Anomaly detection in wireless sensor networks: a survey, *Journal of network and computer applications*, **34**, 1-24.

[4] **Taleb, T. and Kunz**, **A.,** 2012. Machine type communications in 3gpp networks: potential, challenges, and solutions, *EEE Communications Magazine*, **50**, 1-7.

[5] **Ratasuk, R., Prasad, A., Li, Z., Ghosh, A. and Uusitalo, M.A.,** 2015**.** Recent advancements in M2M communications in 4G networks and evolution towards 5G, *Intelligence in next generation networks (ICIN), 18th International Conference*, Paris, 1-6.

[6] **Tan, S.K., Sooriyabandara, M. and Fan, Z.,** 2011. M2M communications in the smart grid: applications, standards, enabling technologies, and research challenges, *International journal of digital multimedia broadcasting*, 1-8.

[7] **Prakash, S. S. and Rao, C. M.,** 2014**.** A comprehensive study of M2M area networks and challenges, *International journal of computer networks and wireless communications (IJCNWC)*, **4**, 1-6.

[8] **Bojkovic, Z. and Bakmaz, M.,** 2013. Machine-to-Machine communication architecture as an enabling paradigm of embedded internet evolution, *Recent advances in computer science*, Serbia, 1-6.

[9] **Bandyopadhyay, S., Balamuralidhar, P., and Pal, A.,** 2013**.** Interoperation among IoT standards, *Journal of ict standardization,* **1**, 1-18.

[10] **Wu, G., Talwar, S., Johnsson, K., Himayat, N., and Johnson, K. D.,** 2011. M2M: from mobile to embedded internet, *IEEE communications magazine*, **49**, 1-8.

[11] **Pereira C. and Aguiar, A.,** 2014. Towards efficient mobile M2M communications: survey and open challenges, *Sensors Journal,* **14**, 1-27.

[12] **Stea, G. and Virdis, A.,** 2014. A comprehensive simulation analysis of LTE discontinuous reception (DRx), *Computer networks journal,* **73**, 1-19.

[13] **Zhang, Y., Yu, R., Xie, S., Yao, W., Xiao, Y. and Guizani, M.,** 2011. Home m2m networks: architectures, standards, and QoS improvement, *IEEE communications magazine*, **49,** 1-9.

[14] **Kotenko, I.**, 2010. Agent-based modeling and simulation of network cyber-attacks and cooperative defence mechanisms, *Computer and information science,* **18,** 1-27.

[15] **Malekzadeh, M., Ghani, A.A., Subramaniam, S. and Desa, J.,** 2011 Validating reliability of OMNeT++ in wireless, *International journal of network security*, **13,** 1-9.

[16] **Michiardi, P.and Molva, R.,** 2012. Simulation-based analysis of security exposures in mobile ad-hoc networks, *European wireless conference*, France, 1-6.

[17] **Raw, R.S., Kumar, M. and Singh, N.,** 2013. Security challenges issues and their solutions for Vanet, *International journal of network security and its applications(IJNSA),* **5,** 1-11.

[18] **Bojic, I., Granja, J., Monteiro, E., Katusic, D., Skocir, P., Kusek, M. and Jezic, G., 2014.** Communication and security in machine-to-machine systems, *Wireless Networking for Moving Objects*, **8611,** 255-281.

[19] **Sapakal R.S. and Kadam, S.S.,** 2013. 5G Mobile technology, *International journal of advanced research in computer engineering and technology* (IJARCET), **2,** 1-4.

[20] **Verma, P.K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., Alsabaan, M., Khalifa, T., Abdelkader, T. and Abogharaf, A.,** 2016. Machine-to-Machine (M2M) communications: a survey, *Journal of network and computer applications,* **66,** 1-27.

[21] **Jung, S., Kim, D. and Kim, S., 2014.** Cooperative architecture for secure M2M communication in distributed sensor networking, *International journal of security and its applications,* **8,** 1-10.

[22] **Bartoli, A.,** 2013. Security protocols suite for machine-to-machine systems, Barcelona, 1-6.

[23] **Cha, I., Shah, Y., Schmidt, A.U., Leicher, A., and Meyerstein, M.V.,** 2009. Trust in M2M communication, *IEEE vehicular technology magazine,* 4, 1-8.

[24] **Prasad, S.S. and Kumar, C.,** 2013. A methodology for an efficient and reliable M2M communication, *International journal of soft computing and engineering (IJSCE),* **3,** 1-7.

[25] **Chaari, L. and Kamoun, L.,** 2011. Performance analysis of IEEE 802.15.4/Zigbee standard under real time constraints *International journal of computer networks and communications (IJCNC),* **3,** 1-17.

[26] **Odabasi, D.S. and Zaim, A.H.,** 2013. A survey on wireless mesh networks, routing metrics and protocols, *Internatıonal Journal of electronıcs, mechanıcal and mechatronıcs engıneerıng,* **2,** 1-13.

[27] **Murty, M.S., Veeraiah, D., and Rao, A.S.** 2012. Performance evaluation of Wi-Fi comparison with WiMAX networks, *International journal of distributed and parallel systems (IJDPS),* 3, 1-9.

[28] **Bakshi, A., Sharma, A.K. and Mishra, A.** 2013. Significance of mobile AD-HOC networks (MANETS), *International journal of innovative technology and exploring engineering (IJITEE)* **2,** 1-5.

[29] **Saproo, D., Goyal, M., Bhagashra, A. and Mahajan, A.N.,** 2013. Analysis of xDSL technologies, *International journal of electronics and computer science engineering*, 2, 1-6.

[30] **Caytiles, R.D. and Lee, S.,** 2015. A survey of recent power line communication technologies for smart micro grid, *International journal of software engineering and its applications*, **9,** 1-8.

[31] **Liu, R. Wu, W. Zhu H. and Yang, D.,** 2011. M2M-Oriented QoS categorization in cellular network, *Wireless communications, networking and mobile computing (WiCOM), 7th international conference*, Wuhan, 1-5.

[32] **Bawiskar, A., Sawant, P. and Meshram, B.B.,** 2013. Wireless security threats, vulnerabilities and their defense mechanisms, *International journal of electronics and computer science engineering*, **2,** 1-10..

[33] **Ugtakhbayar, N., Battulga, D. and Sodbileg**, **S.,** 2012. Classification of artificial intelligence ids for smurf attack, *International journal of artificial intelligence and applications (IJAIA)*, **3,** 1-5.

[34] **Alomari, E., Gupta, B.B., Karuppayah, S., Manickam, S. and Alfaris, R.,** 2012. Botnet-based distributed denial of service (DDoS) Attacks on web servers: classification and art, *International journal of computer applications (0975 – 8887)*, **49,** 1-9.

[35] **Elleithy, K. M., Blagovic, D. Cheng W. and Sideleau, P.,** 2005. Denial of service attack techniques: analysis, implementation and comparison, *Systemics, cybernetics and Informatics journal*, **3,** 1-6.

[36] **Saedy, M. and Mojtahed, V.,** 2011. Machine-to-Machine communications and security solution in cellular systems, *International journal of interdisciplinary telecommunications and networking*, **3,** 1-4.

[37] **Das, R., Karabade, A. and Tuna, G.,** 2016. Common network attack types and defense mechanisms, *Signal processing and communications applications conference (SIU)*, Malatya, 1-5.

[38] **Doh, I., Lim, J., Li, S. and Chae, K.,** 2013. Key establishment and management for secure cellular machine-to-machine communication, *Innovative mobile and internet services in ubiquitous computing (IMIS), Seventh international conference*, Taichung, 1-5.

[39] **Dua, G. Gautam, N. Sharma D. and Arora, A.,** 2013. Replay attack prevention in kerberos authentication protocol using triple password, *International journal of computer networks and communications (IJCNC),* **5,** 1-12.

[40] **Yasodha, M. and Umarani, S.,** 2015. Bandwidth based distributed denial of service attack detection using artificial immune system, *International journal of inventions in computer science and engineering,* 2, 1-9.

[41] **Raza, S., 2013.** Lightweight security solutions for the internet of things, *Postgraduate thesis,* Mälardalen University, Sweden, 1-69.

[42] **Khan, S. and Mauri, L.J.,** 2014. Security for multi hop wireless networks, *CRC press is an imprint of taylor and francis group, an informa business,* U.S, 1-25.

[43] **Report, T.,** 2014. Analysis of security solutions for the oneM2M system, *European telecommunications standards institute,* France.

[44] **Esmailpour, A., Knezevic, V., Gracias, M. and Kokabian, G.,** 2013. Integration of 4g wireless technologies in a test-bed environment, *International journal of wireless and mobile networks (IJWMN),* **5,** 1-14.

[45] **Saleem, K., Derhab, A., and Al-Muhtadi, J.,** 2014. Low delay and secure M2M communication mechanism for ehealthcare, *E-health networking, applications, and services (Healthcom), IEEE 16th international conference,* Natal, 1-6.

[46] **Hoque, M.S., Mukit, A. and Bikas, A.N.,** 2012. An implementation of intrusion detection system using genetic algorithm, *International journal of network security and its applications (IJNSA),* **4,** 1-12.

[47] **Jinwala, D. Patel, D. and Dasgupta, K., 2009.** FlexiSec: A configurable link layer security layer security framework in wireless sensor networks, *Journal of information assurance and security,* **2,** 1-22.

[48] **Lee, S., 2011.** Transport layer security (TLS) implementation for secured mn-ha communication in mobile IPv6, *International journal of future generation communication and networking,* 4, 1-8.

[49] **Manangi, S.J., Chaurasia, P. and Singh, M. P.,** 2010. Analysis of security features in 5 layer internet model, *International journal on computer science and engineering,* 2, 1-5.

[50] **Chavan, A.A. and Nighot, M. K.,** 2014. Secure CoAP using enhanced DTLS for internet of things, *International journal of innovative research in computer and communication engineering,* 2, 1-8.

[51] **UthayaSinthan, D. and Balamurugan, M.S.,** 2013. DTLS and COAP Based security for internet of things enabled devices," *International journal of engineering sciences and research technology,* **2,** 1-6.

[52] **Abarna, K.M. and Venkatachalapathy, K.,** 2012. Light-weight security architecture for IEEE 802.15.4 body area networks, *International Journal of computer applications,* **47,** 1-8.

[53] **OMNET++,** 2014. User manual. *András Varga and OpenSim Ltd,* 1-200.

[54] **INET Framework,** 2015. User manual, 1-160.

[55] **Jung, S., Kim, D. and Kim, S.,** 2014. Cooperative architecture for secure M2M communication in distributed sensor networking, *International journal of security and its applications,* 8, 1-10.

[56] **Olyael, B.I.B., 2013.** Modeling, performance evaluation and suitability study of Zigbee technology for machine-to-machine communications, 1-12.

[57] **Ahmed, H. and Khurram, M.,** 2014. Performance analysis of MAC layer protocols in wireless sensor network, *Information engineering and electronic business journal,* **2014,** 1-9.

[58] **Robin, D., 2014.** Towards automated fault management in smart grid communication networks, 1-89.

[59] **Köpke, A., Swigulski, M., Wessel, K., Willkomm, D., Haneveld, P.K., Parker, T. XVisser, O.W., Lichte, H.S. and Valentin, S.,** 2008. Simulating wireless and mobile networks in OMNeT++ the MiXiM vision, *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems and workshops*, Brussels.

[60] **Chougule, A.A., Vanjale, S.B. and Mane, P.B.,** 2015. Detection and prevention of rogue access point in the 802.11 using various parameters, *International journal of advanced research in computer science and software engineering,* **5,** 1-5.

[61] **Kaur, H., Ebadati, O.M. and Afsha, M., 2011.** Implementation of portion approach in distributed firewall application for network security framework, *International journal of computer science issues,* **8,** 1-11.

[62] **Ray, L.L.,** 2014. A matrix model for designing and implementing multi-firewall environments, *International journal of information security science*, 2, 1-10.

[63] **Stea, G. and Virdis, A.,** 2014. A comprehensive simulation analysis of LTE discontinuous reception (DRX), *Computer networks journal,* **73,** 1-19.

[64] **Dhobale, V.J., Kalyankar, N.V. and Khamitkar, S.D.,** 2014. Computer network performance evaluation based on datarate and number of clients perserver using OMNeT++ Simulation Environment, *Global journal of computer science and technology: E network, web and security,* 14, 1-5.

[65] **Manchikalapudi, V. and Khadar, S.B., 2015.** Simulation of efficiency in mobile Ad Hoc networks using OMNeT++, *Research journal of applied sciences, engineering and technology,* **10,** 1-5.

[66] **Baliga, J., Ayre, R., Hinton, K. and Tucker, R.S.**, 2011. Energy consumption in wired and wireless access networks, *IEEE communications magazine,* **49,** 1-8.

[67] **Jean-Luc**, **S. and Christian, F.,** 2007. Simulation for end-to-end delays distribution on a switched Ethernet, *IEEE conference on emerging technologies and factory automation (EFTA 2007),* 1-4.

[68] **Yagci, A.,** 2011. Comparison and evaluation of routing mechanisms for Wi-Fi mesh networks, 1-64.

CURRICULUM VITAE

Abubakar Karabade, was born 1989 in Bade L.G, Nigeria. Finished Babuje primary school in 2002, and had attended secondary school from 2001-2007 in Government College Nguru, Yobe State Nigeria. Graduate of Computer Engineering from Melikşah University, Kayseri/Turkey in 2014. He has been a Master candidate at the Department of Software Engineering, Firat University, Elazig/Turkey since September 2014.

Contact information

Address: Bida, Bade L.G, Yobe State, Nigeria.

e-mail: karabadeabubakar@gmail.com

Telephone: +905545038803, +2348030551443