PREVENTION AND DETECTION OF DDoS ON WSN

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

INZIMAM UL HASSAN

Registration number

11611820

Supervisor

AMANDEEP KAUR

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

Month November, Year 2017

+

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE548 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0040

Supervisor Name : Amandeep Kaur **UID :** 11384 **Designation :** Assistant Professor

Qualification : M.Tech **Research Experience :** 3 year

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Inzimam Ul Hassan	11611820	2016	K1637	8872399439

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** Amandeep 11/11/17

PROPOSED TOPIC : Prevention and Detection of distributed denial of service attack

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.80
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.60
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.80
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.40
5	Social Applicability: Project work intends to solve a practical problem.	7.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.80

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 3 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 4 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 5 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 6 Name: Aditya Khamparia	UID: 17862	Recommended (Y/N): Yes
PAC Member 7 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): Yes

Final Topic Approved by PAC: **Prevention and Detection of distributed denial of service attack**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal **Approval Date:** 04 Nov 2017

Abstract

The self-configuring type of network in which the sensor node are deployed in such a manner that they can join or leave the network when they want is known as wireless sensor network. The nodes start communicating with each other in order to transmit important information within the network. As this type of network is decentralized in nature, there are numerous malicious nodes which might enter the network. Due to the presence of such malicious nodes, the attacks can be triggered which are classified as active and passive types of attacks. The type of attack in which the raw packets are flood to the victim node is known as DDoS type of attack. It is an active type of attack. When the DDoS attack occurs in the network, it minimizes the lifetime of the network and also increases the overall energy consumption of the network. In order to detect the malicious nodes from the network which cause the DDoS attack, a novel approach is to be proposed in this research work.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation/dissertation proposal entitled "PREVENTION AND DETECTION OF DDoS ON WSN" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Ms. Amandeep Kaur. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

INZIMAM UL HASSAN

R.No 11611820

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled **"PREVENTION AND DETECTION OF DDoS ON WSN"**, submitted by **INZIMAM UL HASSAN** at **Lovely Professional University, Phagwara, India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Ms. Amandeep Kaur

Date: 30-11-2017

ACKNOWLEDGEMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of dissertation. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during this thesis work. I am sincerely grateful to them for their truthful and illuminating views on many issues related to this research.

I express my sincere thanks to my guide **Amandeep Kaur** for his invaluable assistance, motivation, guidance and encouragement without which this research work will be dream. In spite of his busy schedule, he was always there to iron out difficulties which kept o aspiring at regular intervals.

I am really thankful to our **Lovely Professional University** for providing me with an opportunity to undertake this research topic in this university and providing us with all the facilities.

I am highly thankful to my friends and family for their active moral support, valuable time and advice. I am thankful to all of those, particularly the various friends, who have been instrument in cresting proper healthy and constructive environment and including new and fresh innovative ideas during project, without their help, it would have been difficult to complete dissertation within time.

TABLE OF CONTENTS

CONTENTS	PAGE NO.
Title Page	i
PAC form	ii
Abstract	iii
Declaration by the Scholar	iv
Supervisor's Certificate	v
Acknowledgement	vi
Table of Contents	vii
List of Abbreviations	ix
List of Figures	x
CHAPTER 1	1-10
INTRODUCTION	1
1.1 WIRELESS SENSOR NETWORK (WSN)	1
1.2 CHALLENGES IN WSN	2
1.3 WSN ISSUES	4
1.4 ATTACKS IN WSN	**7**
1.5 TYPES OF DISTRIBUTED DENIAL OF SERVICES	8

TABLE OF CONTENTS

CONTENTS	PAGE NO.
1.6 MOTIVATION	10
CHAPTER 2	11-13
REVIEW OF LITERATURE	11
CHAPTER 3	14-17
PROPOSED WORK	14
3.1 SCOPE OF THE STUDY	14
3.2 OBJECTIVES	14
3.3 RESEARCH METODOLOGY	15
3.3.1 TOOL DESCRIPTION	15
3.3.2 FLOWCHART	16
3.4 EXPECTED OUTCOMES	17
CHAPTER 4	18
CONCLUSION	18
4.1 CONCLUSION	18
REFERENCES	19-21

LIST OF ABBREVATIONS

DoS	Denial of Service
DDoS	Distributed Denial of Service
WSN	Wireless Sensor network
MAC	Medium access control
IP	Internet Protocol
BS	Base Station
QOS	Quality of Service

LIST OF FIGURES

FIGURE NO.	FIGURE DESCRIPTION	PAGE NO.
Figure1	Traditional wireless sensor network	1
Figure2	Major issues in WSN	5
Figure3	DDos attack in WSN	

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Network (WSN)

There are numerous sensor nodes deployed within a wireless sensor network (WSN) along with one base station in it. The sensor nodes are small sized devices which have very less power, and cost along with constrained memory, computational and communication resources. There are numerous spatially distributed autonomous sensors present within the network which gather the information from their surroundings and pass it to the base station.

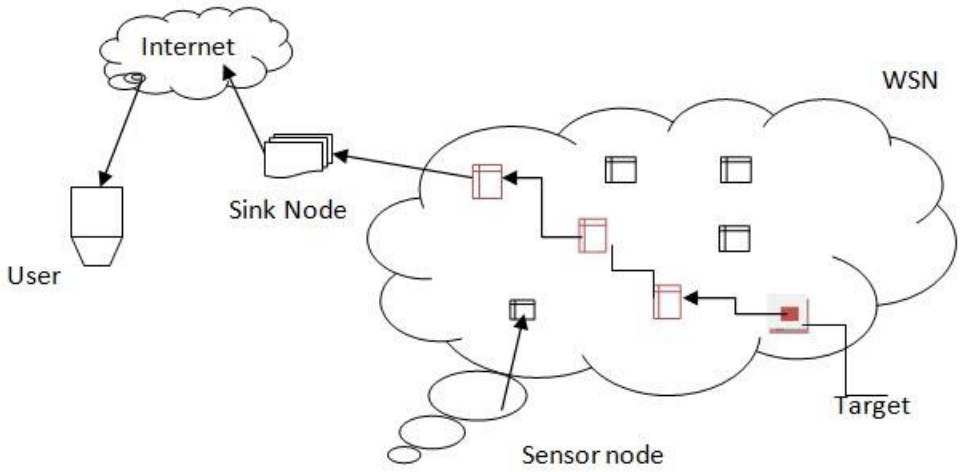


Fig.1 Traditional Wireless Sensor Network [1]

The nodes deployed within these networks collect the information from surrounding environmental areas. All the gathered information is transmitted to the base station present in the network which acts as a gateway amongst the sensor networks and the external environment. The storage capacity of base stations is very high and it also consists of numerous data processing capabilities which can be useful in the network [2]. The transmitting of important information which is received from the sensor nodes by the base station is its major task. This information can be accessed by the end user and can be utilized as per its requirement. Within the area of base station basically the sensor nodes are deployed which can form groups as per the requirement of the application. Due to the smaller sizes of the sensor nodes, the sizes of their batteries are also small. Due to this, the batteries of the sensor not deplete very easily and cannot be recharged easily as they are deployed in very large areas. Thus, the lifetime of the network reduces which is a major concern.

The information that is achieved through the continuous monitoring of the nodes is forwarded to the base station due to which these networks are known as bi-direction wireless sensor networks. Within the scenarios which require continuous monitoring, and it is not possible for the humans to monitor the surroundings, which can be possible by deploying the wireless sensor networks. There are many unique properties of the wireless sensor networks such as the batteries have limited life time; the sensor nodes are heterogeneous in nature, the nodes are mobile and so on. Initially, the military application utilized the WSNs within them in order to monitor the health and military applications. Further, as per the growth in these technologies, various other applications were also involved such as automatic manufacturing, home automation, robot control and so on. On the basis of the information of temperature gathered from the surroundings by sensor nodes, the forest fires were also detected within various applications.

1.2 Challenges in WSN

There are numerous technical issues which arise during the deployment of wireless sensor networks. Some of these issues were given below:

- **Ad hoc deployment**: Within various areas which are infrastructure less, large numbers of sensor nodes were deployed. The sensor nodes were distributed within the specific regions through various methods. The connectivity as well as distribution of these nodes was done by the nodes themselves due to which they are also known as self-configuring in nature [3].

- **Unattended operation:** There is no need of providing any human interaction within the WSNs once the nodes are deployed in the network. The nodes are self-configuring in nature and can also adapt themselves as per the changes occurring within these networks

  [4].
- **Untethered**: There is no connection of the sensor nodes to any external energy source within these networks. Within the sensor node there is limited energy available which is utilized during the processing and communication amongst the sensor nodes. The processing within the energy consumption is dominated by the communication. There should be minimization in the energy consumption to the utmost possible level in order to utilize the overall energy present in the network in proper manner [5].

- **Dynamic changes**: The nature of wireless sensor networks is highly dynamic and keeps changing. The sensor nodes present within the network can easily adapt to these changes when higher number of nodes enter the network or in case there is a node failure in the network.

- **Fault tolerance:** The maintenance of network in such a manner that the failure of one node does not affect the performance of the complete network is known as fault tolerance. In order to ensure this, there are numerous adaptive protocols introduced in these networks.

- **Security issues:** There is an increase in the threats and attacks in WSNs in order to breach their security. Further, due to the wireless connectivity as well, the attacks can be caused. Due to the reason that there is an unguided transmission medium which is highly susceptible to the security attacks, the wireless networks are highly prone to various types of security attacks in comparison to the other networks. In order to eavesdrop, the direct candidate can be used due to the broadcasting nature of the wireless communications occurring here. Within the wireless ad hoc networks, majority of security issues as well as threats were identified which are to be resolved through numerous techniques [6].

- **Synchronization and Localization:** The data that is gathered from all the nodes can be useful to various applications. Thus, the synchronization of these nodes is very important. Within the wireless sensor networks, the clock synchronization is a very important factor. Within the nodes present in the network, the clocks are provided due to which the time is synchronized within these networks. The data is directly prepared and broken down with the help of worldwide clock present within the sensor framework. This helps in predicting the future framework required within these networks. There are also many other issues present in the network such as the transmission delays. The synchronization of nodes is also thus not possible due to the absence of any broadcasting clock within the network.

  An important test within the sensor networks is the localization of the sensor nodes which use the relative positions of the sensors. Thus, numerous methodologies have been proposed in order to solve all such issues. In order to increase the precision within the networks, the distributed algorithms also play a very important role within these networks.

- **Short Range Transmission:** In order to minimize the possibility of eavesdropping, a node, the short transmission range has to be considered within the WSNs. This helps in minimizing the possibility of eavesdropping. In order to provide point to point transmission amongst the nodes, higher transmission power is required within the long range transmissions. This is the reason that there is an increase in chances of a packet being eavesdropped within the network [7].

- **Energy consumption:** Within the WSNs, energy consumption is a major issue. There is limited amount of energy present within the sensor nodes as they are small in size. The batteries are present within the network which are small and

are not easy to be replaced. Thus, various power-related protocols as well as algorithms have been proposed by numerous researchers in order to solve this issue.

1.3 WSN Issues

The design and performance of wireless sensor networks can face numerous isues amongst which some are listed below [8]:

i) Energy conservation

ii) Security iii) Self-Organization

iv) Time synchronizati on iii) Quality of Services (QoS) iv) Node localization

Energy consumption is one of the major issues which have to be considered while proposing the design of hardware and software within the WSNs. The practical applications of WSN are sometimes questioned due to the problems arising as a result of energy consumption. Synchronization, architecture, data collection, security and numerous other issues also are important here which need to be resolved by taking numerous measures during the designing of wireless network. Here, all such issues are to be discussed in order to understand the various scenarios which might occur in the network.

The factors due to which the performance of the WSNs can be affected are:

i) Energy conservation: In order to perform numerous operations within the wireless sensor networks, the basic requirement is power [9]. Within numerous activities such as gathering or data, its processing and communication require energy. Even when the nodes are not performing any tasks, there is a need of huge amount of energy in the components of nodes when some dedicated operations are to be performed. Once, the energy of the

nodes is consumed completely, the batteries of these nodes need to be changed or recharged. However, as the nodes are deployed in large areas where it's not possible for the humans to go, the replacement of these batteries is almost impossible. Thus, within the design and development of wireless sensor networks, this issue is very major. The energy efficient hardware and software protocols are proposed which are applied within these networks.

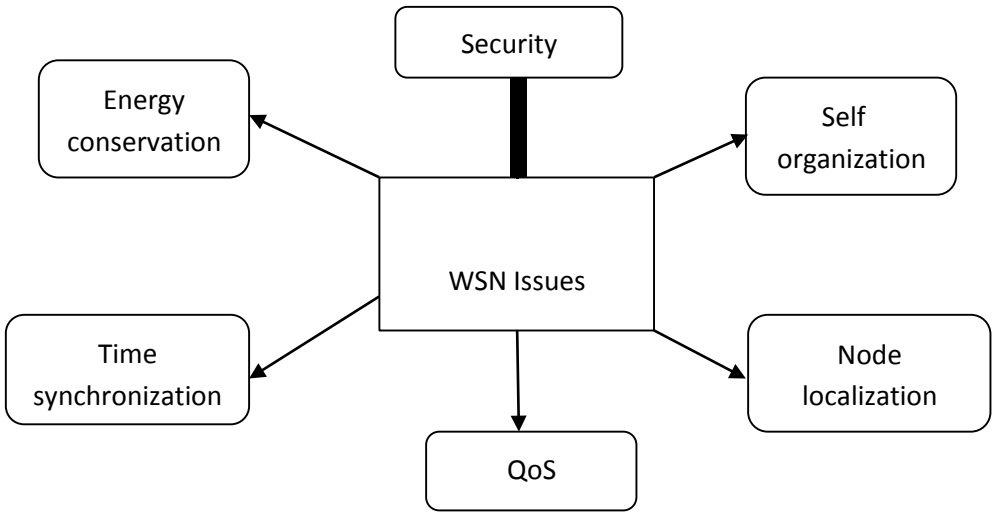


Fig. 2: Major Issues in WSN

ii) Security: Another challenging issue within the designing of WSN is the maintenance of security of these networks. Not only within the military applications but also in the huge buildings in order to provide alarms and monitor the surroundings, the WSNs are deployed. Similarly these networks are also deployed on the airports as well as in hospitals in order to ensure the safety of the patients [10]. There is a need to protect the information which is basically travelling amongst the sensor nodes of the network or amongst the sensors and base stations. If no preventive measures are taken here, the network might face an eavesdropping attack. It becomes extremely important that every single node and base station in sensor networks are able to keep a check that the data received is not a false data and is sent by a trusted sender not by any attacker. The way of prediction of a network can be changed by false data. It is important that the data which reaches to the end user must not change at all and its integrity needs to be fully maintained. The way of prediction of any network can be changed by fake/false data.

iii) Self-Organization: In WSN, the independence and flexibility of each and every sensor node is highly important. The nodes must have an ability to heal and organize themselves as per various situations. The different techniques of topology and deployment

need to be managed by the nodes themselves as there is no set infrastructure for the management of network.

iv) Time Synchronization: At the time of execution, there is a demand of time synchronization by many WSN applications. If there is a collaborative sensor network then to track applications it may require group synchronization.

v) Quality of Service (QoS): Reliability, data delivery and energy conservation are few parameters which can be used to define the quality. The QOS is the amount of service quality offered to the user by any application. QOS is used to enhance signal transmissions or to improve field coverage. It is highly important to examine the quality of services and coverage uniformity on a regular basis. If we take a ratio of area covered by sensors to total area then the result would be QOS. The consumption of energy by nodes which consume low power can be used to calculate QOS.

vi) Node localization: This is another one of the most important techniques in wireless sensor networks. The place estimation can be differentiated into two methods. First is source localization and the second one is node-self localization. In few particular cases of target localization, energy dependent methods can also be used. Because of the wide range of applications which use localization methods some challenges arise during their use. Several evaluation criteria's are used for localization in WSN. Self-localization is the process of locating the unknown location of a node. There is a large number of inexpensive nodes which are deployed in a dense way to evaluate different phenomena. To determine the exact location of the target is the most important and prime objective.

1.4 Attacks in WSN: There are number of attacks in WSN some of them are given below:

- **Wormhole**: This is a type of attack in which there is a formation of a tunnel by the malicious nodes and it is kept hidden from other legitimate nodes. This tunnel is used to send data packets from one malicious node to other. A malicious node in one area attracts the packets from its area and transmits them to the malicious node of other area. There are various ways like in-band and out of band ways for the creation of a tunnel. This kind of attack can put a very huge effect on the procedure of routing and localization as there is no need to make any changes in other genuine networks to trigger this attack. Different techniques like packet relay, high power transmission, wormhole using encapsulation, out of band channel can be used to establish this attack.

- **Blackhole:** This is again a very dangerous kind of attack as in this attack re-programming in different set of nodes can be done by the attacker. This may lead

to the blockage of packets or the attacker can do anything else with the captured packets like generating false messages but does not forward them to the base station in WSN.

- **Sybil attack:** Sybil attack is an attack in which a malicious node can reshape itself like other different nodes. Multipath routing distributed systems are very prone to this attack as they have no centralized entity which can be used to verify the identity of each node.

- **HELLO flood attacks**: In this kind of attack, HELLO packets are used to influence different nodes in the network. With the help of HELLO packets the malicious nodes manage to introduce themselves to neighboring nodes. The receiving node sometimes believes that it is within the radio range of the sender but sometimes the HELLO packets

  are sent at an extremely fast speed by the malicious node that the receiving node tends to believe that they are being sent by their neighboring node. Due to this, when the nodes send the messages to the base station, the messages are sent through malicious node.

- **Denial of Service (DOS) attack**: There are various types of DOS attacks which can be triggered at different layers but the primary motive of these attacks is to temporarily make the network resources unavailable. If we talk about an example then at network layer it can result into homing or misdirection and at transport layer it can be performed by flooding. The complete programming of the sensors can be manipulated by the attackers. The attackers can be so influential that they can even place a false sensor in place of a legitimate sensor resulting the modification of whole circuitry.

- **Distributed Denial of Service (DOS) attack:** The purpose of this attack is to prevent authentic users from using website, web service or computer system like specified network resource. It is a coordinated attack of given target network or system availability. This attack is indirectly launched through many compromised computing systems. The secondary victims are those that are used to launch the compromised systems and primary victims are those that attack the services.

The attacker in a DDOS attack attains the capability of carrying much stronger attack while remaining unknown by the use of secondary victims because it becomes very tough for network forensics to eliminate and detect the actual attacker.

1.5 Types of Distributed Denial of Service attacks

The term jamming is used to define an attack in which the transmission of a radio signal is interfered by radio frequencies which are being used by sensor network. Jamming can be of two types: In Distributed Denial of service attack, the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming [17]. Jamming may come in two forms:

- **Constant jamming:** This type of jamming implies the jamming of the entire network.
- **Intermittent jamming:** In this, messages are periodically exchanges by sensor nodes.

The communication protocols can be intentionally violated by attacker in link layer, e.g., ZigBee or IEEE 802.11b protocol and in order to attempt collisions messages are continuously transmitted. The packets lost by collision are needed to retransmit. By refusing routing messages a multi-hop network advantage is taken by node in routing layer. The conclusion is that any node that is affected by attacker will not be able to exchange messages with the part of network. In case of flooding, that transport layer is also affected by attack. Number of connection requests is send to malicious node in case of flooding. The connection requests are handled by allocating resources.

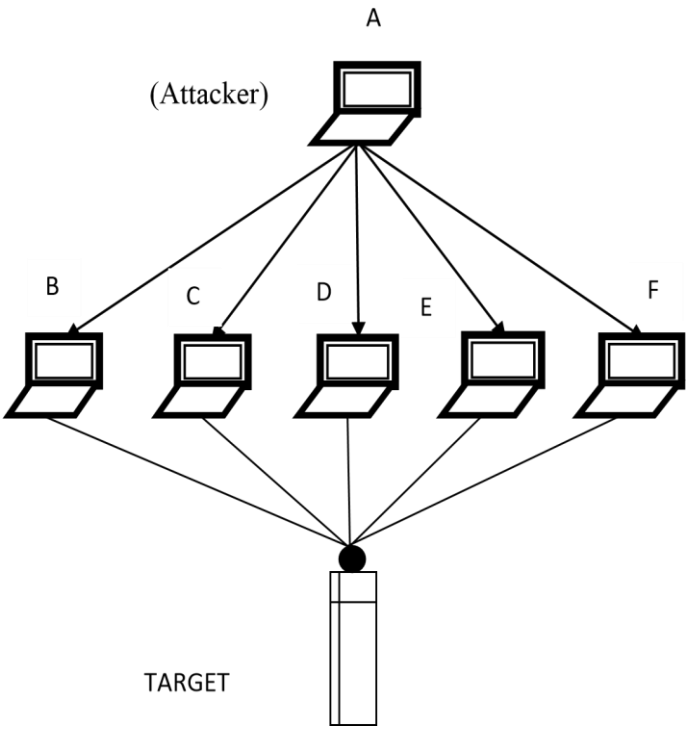


Fig. 3: DDoS attack in WSN

In this attack excessive amount of packets are sent are sent to a server to slow down its pace or to make the scarcity of resources to the users so that a user can not access the facility. The Fig. 3 shows the diagram of Distributed Denial of Service attack. It consists of six nodes or computers name as A, B, C, D and E. In this kind of harmful attack, an attacker i.e. computer A will send request or packets to compromised computers say computer B, C, D, E, F and then the server is flooded with thousands of unwanted requests. And hence user can't access the resources [17].

1.6 Motivation

The Wireless Sensor Network is the self-configuring network and it is used to sense the environmental conditions like temperature and pressure. Due to its decentralized nature, security is the major concern of this network. The security issues can increase the energy consumption of the network and reliability of WSN. To improve performance of WSNs the technique is required which detects malicious node from the network.

CHAPTER 2

LITERATURE SURVEY

Varsha Nigam, et.al, (2014), has concluded that for working in critical conditions, WSN has proved out to be a good and reliable technology. The sensor networks can be deployed at various places such as war zones, buildings or traffic surveillance. If we talk about one major challenge in the use of wireless sensor networks then it can be the security issues. In this paper, authors have proposed a profile based protection scheme (PPS security scheme against DDoS (Distributed Denial of Service) attack. Flooding of excessive data is the major cause of this kind of attack because of which the bandwidth of the network is completely consumed by data delivery which affects the overall performance of the network. [18]. The main aim of authors is to visualize the effect of DDoS attack in network and identify the nodes that affect the performance of network. The PPS blocks the attack initiated by the attacker by checking it through profile based security scheme. A performance metrics can be utilized to evaluate the performance of the network. If the simulation results represent the same performance in case of normal routing and in case of PPS scheme, it means that the PPS scheme has worked with complete efficiency and shows 0% infection in presence of attacker.

Raksha Upadhyay, et.al, (2015), have recommended that wireless network with sensing and processing information merit is known as wireless sensor network (WSN). WSN consists of small sensor nodes with transducer, battery, microprocessor along with storage media. This is prove to be economical and simple solution for different applications. The WSN have open nature that leads it to be affective for different security threats. In network, the information and sensor node information is compromised due to different security attacks such as black hole, wormhole attack, DDOS attack, etc. The goal of DDOS attack is to infect the network by the drainage of resource capability. Meaningless messages in large numbers are sent by the attacker to increase the network congestion and also degrade the life of node and network. The life of network is directly proportional to battery capacity that draining in battery energy directly degrades the life of node. In this paper [19], severe problems have been observed by authors and a solution is proposed a solution to overcome the problem of power draining due to DDOS attack. In order to simulate and evaluating the performance of proposed solution for AODV and DSR routing protocols in WSN they have used Qualnet 5.0 simulator.

Raksha Upadhyaya, et.al, (2016), have analyzed that open nature of wireless sensor networks (WSN) results in more vulnerability to outside attacks. Different attacks such as denial of service, black hole and sink hole highly affect the overall output of the network. DDOS attacks the most dangerous attacks which greatly harm and hamper the complete working of the network. Distributed denials of service (DDOS) attacks are attacks that are launched by a set of malicious entities towards a node or set of nodes. In this paper [20], authors have proposed a solution to prevent WSN from DDOS attack. In proposed solution they have used dynamic source routing (DSR). The concerned nodes energy is used for detecting and preventing attacks. The proposed scheme provides a modified DSR with security aware mechanism for DDOS attack. The whole process is carried out in four steps. The DDOS attack is prevented by examine battery charge of each node that provides identification of malicious node. Since a sensor network does not have any blacklist to detect malicious nodes therefore a shutdown method can be applied to ignore malicious node in the network. This will help in removing the malicious node from communication and start transferring packet transmission from alternative routes. The proposed scheme is implemented using Qualnet 5.2 simulator.

Taranpreet Kaur, et.al, (2016), have analyzed that Wireless Sensor Networks (WSNs) is a collection of large number of sensor nodes that have limited capabilities for collecting sensitive information. There is advancement in this technology that leads to security as major concerns. In WSN, there are number of attacks like Distributed Denial of Service (DDOS) attacks. In case of this attack, many attacks are adapted by malicious node such as flooding attack, black hole attack and warm hole attack in order to disturb the overall functionality of network. When it is used in military and industrial applications the risks are more. The constraints in WSN are limited battery power, low capabilities of nodes etc. The challenge for researchers is to present a security model that will consider these constraints and provide security. In order to detect and prevent DDOS attacks, number of researchers has proposed new mechanisms. In this paper [21], authors did a survey on different existing approaches on basis of various parameters. This survey will help researchers to improve the existing techniques that have low false alarm problem and less energy consumption.

Shital Patila, et.al, (2016), have analyzed that Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission. There are some weaknesses in WSN that results in that there sensor nodes are more vulnerable to most of the security threats. The most popular attack that effect sensor node is Denial-of-Service (DoS) attack. So, there is need to prevent Dos attack using different techniques. There are number of techniques that have been used by different researchers for preventing DDoS attack. In this paper [22], authors have proposed an improved Co-FAIS immune system for DoS attack in WSN. Co-FAIS immune system is the first real time intrusion

detection model that compares current system with normal system to recognize the attack by using fuzzy logic. But it has some disadvantages such as lacks in learning capabilities and based on single normal model which does not change over the time during detection. So, authors have improved the current Co-FAIS system by adding two learning parameters in fuzzy system that helps in improving the accuracy rate of detection and improves learning capabilities. The simulation results show that the proposed system will improve the accuracy rate of attack prevention, reduce the false alarm rate that helps in recognizing different DoS attack.

CHAPTER 3

PROPOSED WORK

3.1 Scope of the Study

The wireless sensor network is the decentralized network in which sensor nodes can join or leave the network whenever they want. Due to its decentralized nature, many nodes can join or leave the network when they want. In the network, sometimes, the malicious nodes enter which can generate the active and passive types of attacks. The active attacks are those which affect the network's performance and the passive attacks are those which do not affect the performance of network. The DDoS attack is the Distributed Denial of Service attack in which malicious node selects some of the nodes which can flood the victim node. The malicious node also spoofs the credentials of the legitimate node. In this research work, the technique will be proposed which detects and isolate malicious nodes from the network which are responsible to trigger DDoS attack in the network.

3.2 Objectives

1. To study and analyze various techniques for isolation of DDoS attack in WSN.

2. To proposed improvement in mutual authentication technique for the isolation of DDoS attack in WSN.

3. The proposed improvement will be based on the threshold technique for the detection of malicious nodes in the network.

4. Implement proposed technique and compare it with existing in terms of various parameters.

3.3 Research Methodology

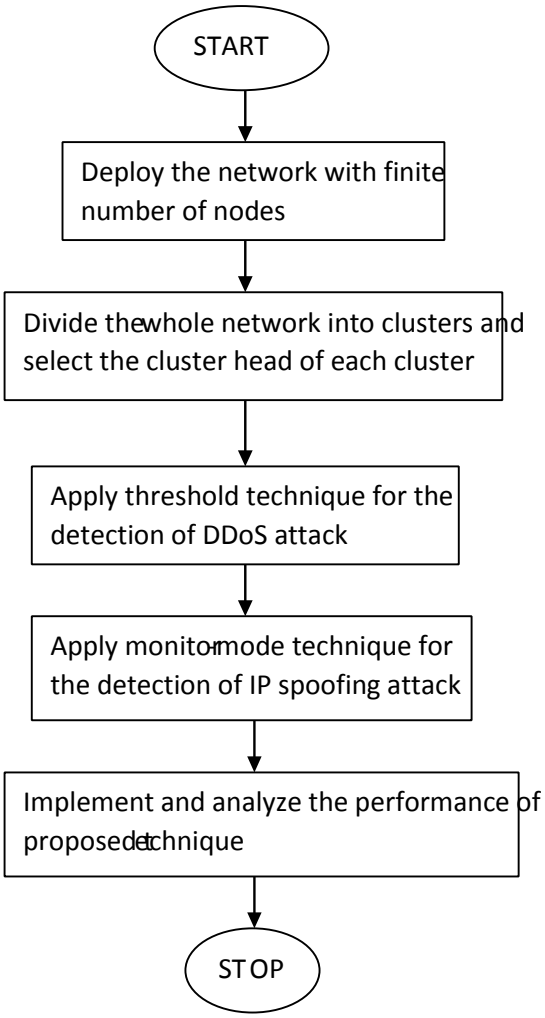
3.3.1 Tool Description:

NS2: In order to analyze the performance of the model that is deployed by the researcher, the simulation is performed. It helps in computing the performance of the proposed technique when it is applied in real time scenario. There are two types of simulators. They are event based and time based simulators. An event based simulator in which the generated events are triggered within a certain time duration is known as network simulator version two. The network models are simulated with the help of this network simulator. There are some latest versions derived for this network simulator with the advancement in research. The version with higher compatibility with Ubuntu 12.04 is NS2-2.35. Both text and animation based simulations are performed within this simulator. There are two outputs generated when the object oriented language is executed. The initial output is the .tr file which is also known as the trace file. Here the text base simulation is saved within this output. Further, the second output is in the form of .nam file. This results in providing animation based simulation. There are numerous applications that utilize this simulator as there is no other simulator which can provide both text-based and animation based simulations for various applications.

An active attack that is responsible for dropping the data and control packets within the network is known s the selective forwarding attack. There is a minimization of performance of network in terms of various parameters when a malicious node is present within the network. The parameters such as energy consumption, throughput and delay define the performance of the network which can change as per the modifications made within the network. In this work, in order to recognize and remove the malicious nodes from the network, a technique has been proposed. On the basis of traffic analyzer and threshold values present within the network, there is a technique proposed. The central controller is chosen within the network depending on the trust values of the nodes. Depending on the data packets that are re-transmitted within the network, the trust value of the node is computed. There is a central controller node that registers each node according to IP, MAC address and the current data. The bandwidth required for communication related to the base station is assigned using the central controller node.

Depending on the hop count and sequence number, a secure and efficient path is generated from sensor node to base station. The data is transmitted from the sensor node. Further the central node checks individually each node in a random manner. The nodes that have threshold unequal to the decided threshold value are to be detected and presented as malicious node within the network. For removing such malicious nodes from the network, a multipath routing method is presented here.

3.3.2 FLOWCHART



3.4 Expected Outcomes

Following are the various expected outcomes of this research:

1. The DDoS attack reduces the network efficiency by flooding the network with raw packets. This leads to increase energy consumption of network and reduce network lifetime. The proposed improvement leads to detection of malicious nodes which increases the network lifetime.

2. When the DDoS attack triggers in the network, the network throughput is reduced and packet loss increases. The proposed improvement increases the throughput and reduces packet loss in the network.

CHAPTER 4
CONCLUSION

4.1 Conclusion

In this research work, it has been concluded that Wireless Sensor Network is the self-configuring network due to which some malicious nodes enter the network which are responsible to trigger active and passive attacks in the network. The DDoS attack is the Distributed Denial of Service attack in which the malicious nodes flood the victim with the raw packets. The technique of threshold will be proposed which detects and isolated malicious node from the network. The proposed improvement leads to increase network lifetime, throughput and reduce network delay.

REFERENCES

[1] Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "Issues and Challenges in Wireless Sensor Networks", IEEE International Conference on Machine Intelligence Research and Advancement, vol 4, pp.58-62, 2013.

[2] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[3] Gouvy, N., Hamouda, E., Mitton, N., & Zorbas, D., "Energy efficient multi-flow routing in mobile Sensor Networks", IEEE In Wireless Communications and Networking Conference (WCNC), vol. 3, pp. 1968-1973, 2013.

[4] Kaur, K., & Kumari, N. Evaluation and Analysis of Active RFID Protocol in Wireless Sensor Networks, vol. 3, pp. 121-129, 2010.

[5] Jiang, L., Bing Fang, & Li., "Energy optimized approach based on clustering routing protocol for wireless sensor networks", CCD Conference. IEEE, vol. 5, pp. 181-190, 2011.

[6] Wang, Y., & Guo, S., "Optimized energy-latency cooperative transmission in duty-cycled wireless sensor networks", In Mechatronics and Automation (ICMA), 2013 IEEE International Conference on, vol. 5, pp. 185-190, 2013.

[7] Neamatollahi, P., Taheri, H., Naghibzadeh, M., & Yaghmaee, M., "A hybrid clustering approach for prolonging lifetime in wireless sensor networks", IEEE In Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on, vol. 6, pp. 170-174, 2011.

[8] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in wireless sensor networks", WCE, vol.1, pp 5-15, 2008.

[9] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[10] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, pp. 14-27, 2010.

[11] M.K. Jain, “Wireless Sensor Networks: Security Issues and Challenges”, International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.

[12] A.K. Pathan, “Security in Wireless Sensor Networks: Issues and Challenges”, Proc. 8th International Conf. Advanced Communication Technology, vol. 2, pp. 1043-1048, 2006.

[13] Patel MM, Aggarwal A, “Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET)”, 2016 International Conference on IEEE, vol. 5, pp. 2109-2112, 2016.

[14] Krishnan NS, Srinivasan P, “A qos parameter based solution for black hole denial of service attack in wireless sensor networks”, Indian J Sci Technol, vol. 9, pp. 1001-1010, 2016.

[15] Healy M, Newe T, Lewis E, “Security for wireless sensor networks: A review in Sensors Applications Symposium (SAS)”, 2009 IEEE, vol. 3, pp. 80-85, 2009.

[16] Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamali, “Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network”, International Journal of Computer Applications Technology and Research vol.3, pp. 541 – 546, 2014.

[17] Priyanka Goyal, Sahil Batra, Ajit Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications, vol.9, pp.11-15, 2010.

[18] Varsha Nigam, Saurabh Jain, Dr. Kavita Burse, “Profile based Scheme against DDoS Attack in WSN”, IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies, vol. 5, pp. 112-116, 2014.

[19] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt, “Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain”, 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), vol. 3, pp. 446-451, 2015.

[20] Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia, “DDOS Attack Aware DSR

Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74, 2016.

[21] Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma, "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), vol. 4, pp. 131-140, 2016.

[22] Shital Patila, Sangita Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, pp. 715-721, 2016.