Advances and Applications in Mathematical Sciences
Volume 18, Issue 8, June 2019, Pages 567-585

A TECHNIQUE FOR IDENTIFICATION AND MOLLIFICATION OF GREEDY NODES IN WIRELESS MESH NETWORKS (WMNs)

AFSHAN HASSAN and RAJEEV SHARMA

Computer Science Engineering
Chandigarh Engineering College
Mohali (Punjab), India
E-mail: wani.afshan786@gmail.com
rajeev.3564@cgc.edu.in

Abstract

Wireless Mesh networks (WMN's) are prone to a number of attacks & these attacks compromise the security of these networks. Attaining security in these networks is a challenging task. It is logical to consider that there are many types of scripts in the internet. The virus can either be a key logger or somebody else's mischief. With this script we can steal any information. Since the existence of virus cannot be ignored, therefore the author have tried to present their work on first detecting it and later on fixing it. We have arrived at many pubs and we are looking at some ways in which we can save the user. In this paper, we have come up with a methodology to first detect the selfish node in the network and later on provided a technique for mitigation of the same. NS2 simulator has been used to simulate and analyze the performance of our proposed methodology for Open Shortest Path First(OSPF) protocol in WMN's.

I. Introduction

Wireless Mesh Networks (WMN's) consist of Wireless Access points (AP), Mesh routers (MR's) and Mesh clients (MC's) (Figure 1). Multiple mesh routers can be connected together through these access points. Access points are responsible for connecting clients in wireless mesh networks through mesh routers. They also connect the WMN's to the core network. Mesh routers are responsible for transmitting information among mesh clients. Mesh clients are the end devices that access the network [1].

2010 Mathematics Subject Classification: 68M10.

Keywords: Wireless Mesh Networks (WMN's), Distributed Denial Of Service (DDoS), covert channel, Media Access Control (MAC), Open Shortest Path First (OSPF), Switch port analyzer, Intrusion Detection Systems (IDS), Packet Delivery Ratio (PDR).

Received February 11, 2019; Accepted March 17, 2019

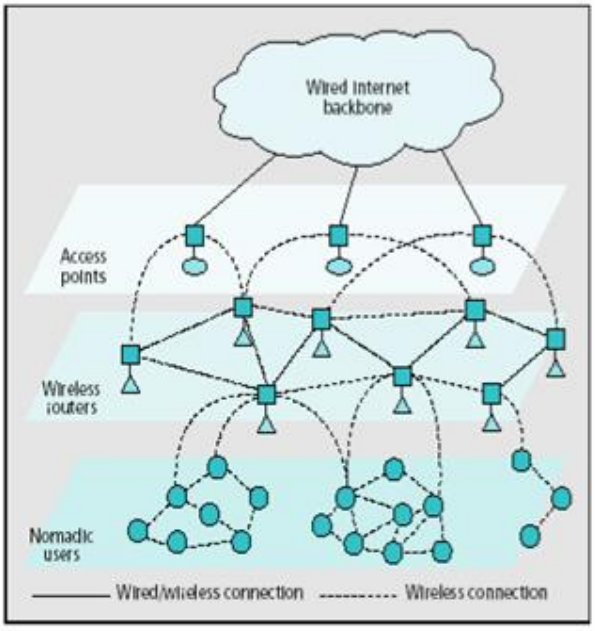

Figure 1. Architecture of wireless mesh network.

With the advent of Wireless Mesh Networks (WMNs) as one of the poignant technologies dominating the world of wireless networking while providing a variety of benefits including seamless and flexible connectivity to the networking nodes anywhere in the world at any time, WMNs also bring on front glaringly inescapable and vulnerable issues compromising the security because of their unique features [2]. As a result of discernible security requirements of WMNs, they require conspicuous resources [3]. The necessity of having different levels of security services in WMNs arises because of their capability to provide different types of services related to networks. Also since WMNs are able to harness different resources in the network which in turn raises the importance of having different security levels in WMNs. The paper has been organized as follows. Section II discusses characteristics, security challenges and issues in WMNs. Section III explains the work related to our research. Section IV introduces the problem statement. Section V discusses the objectives. Section VI discusses the proposed solution. Proposed methodology and simulation results are discussed in Section VII and Section VIII.

II. Characteristics, Security Challenges and Issues in WMNs

(A) Characteristics of Wireless Mesh Networks:

1. **Self organization and self configuration:** Nodes can be added to or deleted from the network after the network is organized for further extension of the network.

2. **Reliability**: WMN's are reliable. In the event of a node failure, they easily adapt to the change & can even route the packet through the alternate path.

3**. Adaptability**: With the addition or subtraction of nodes, the network performs well.

4. **Point to point connection:** The packet can be routed directly from source node to the end node without its need to travel through intermediate nodes.

5. **Multihop**: WMN's are wireless multihop networks. Every node in a WMN can transmit data from one end to the other & can ensure optimal path selection from source to destination.

(B) Security Challenges in WMN's [1]

WMN's are prone to both active as well as passive attacks. Confidentiality of mesh networks is compromised as a result of passive attacks on the network whereas authentication, non repudiation, integrity & availability of the mesh networks get infringed because of active attacks. Some of the focal points that make it difficult to ensure security in these networks are listed below:

1. The enormous number of wireless channels expose mesh networks to different types of attacks thereby compromising the security as a whole.

2. The placement of routers in a mesh topology is of grave concern. These routers are placed anywhere in buildings or surroundings to ensure robust communication. This makes the network prone to attacks from inside as well as outside.

3. WMN's are prone to change. This can cause mistrust in the relationship between nodes of wireless mesh networks. There are three serious security challenges faced by the mesh architecture.

1. Detection of damaged node: This involves four main attacks:

The simplest attack involves replacing a node in WMN. In order to collect important data related to the defective node we need to consult the neighboring nodes whenever topology of the network changes.

The second type of attack snoops on the node to capture information from the node. This type of attack is very difficult to detect because it does not involve alteration of original data.

The third type of attack involves modifying the internal routing algorithm of the network, thereby changing the topology of the network.

The fourth type involves replicating a node & putting those replicated nodes at deliberately chosen locations in the WMN layout. This enables an attacker to insert fake data into the network.

2. Multihop routing: Here the routing algorithms operating inside WMN need to be guarded from attack. The attacker attacks the routing algorithm, thereby degrading the performance of the network.

3. Fairness: Achieving fairness in a network is a challenging task. Fairness in a network implies that no node in the network experiences starvation of data.

(C) Handling Security Threats and Privacy

This section deals with explaining how various issues related to privacy including different internal as well as external threats are dealt within our posited research proposal.

(i) Security and Privacy Requirements

Various parameters related to security and privacy should be perceived to ensure secure communication in WMNs [3].

(ii) Confidentiality [4]

Data confidentiality dictates that only the two communicating entities can read the interchanged data. To ensure this our proposed scheme uses encryption along with key-pair LKMN while interchanging data. In order to shield the network from compromised nodes, these link key-pairs are renewed either regularly or on an on-demand basis thereby securing the network.

(iii) Integrity [5]

When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. Message authentication code (MAC) used with each message, assures the integrity of the exchanged data. In our proposed scheme we have used keyed-Hash Message HMAC (hashed MAC) or KHMAC (Keyed-hash MAC). As a result, any message altered by an opponent can be detected at next-hop node or at the receiver's end. In order to guarantee the delivery of the message, a mechanism for multi-route delivery (Figure 2) is employed.

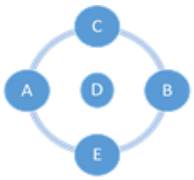

Figure 2. Message Integrity of Mesh Networks.

(iv) Authenticity [6]

Authentication helps establish proof of identities. The sending node while sending messages to the corresponding node includes a hash chain element within the message, which when received by the corresponding node is responsible for authentication. The current message received from a particular sender is authenticated by taking hash of the hash-element associated with that message and then comparing it with the previous message from the same source.

Various schemes and protocols have already been proposed for WMNs, but they usually suffer from one of the following drawbacks:

- They perform end-to-end authentication only. Hence, fabricated packets can merely be rejected at the destination nodes.
- A trusted authority (TA) for authentication and key distribution is usually required. WMNs lack any centralized trust.
- Before deploying dynamic WMNs, keys should be distributed in advance, which is infeasible for such networks.

- Confidentiality can be achieved through asymmetric cryptography which is computationally complex.
- Only external nodes are considered to be the source of attacks, whereas internal nodes are assumed to be benign This is clearly a disadvantage if the internal node is compromised anyhow.

III. Literature Survey

A number of attacks happen in the real time networks and these attacks get the entire network information [7]. This paper aims to identify the various attacks executed in OSI Model and to fix them with some solution. The network attacks can be categorized into four types, Wormhole attack is one of the types of Network Layer attack. The proposed methodology had implemented a method wherein notification was sent to every node, if the threshold increased beyond the limit. The Wormhole attack was one of the dangerous attacks in the Wireless Sensor Networks because it was independent of the MAC Layer. In the Wormhole Attack, the attacker creates a fake link between a user and the malicious node, the normal user predicts that it was high speed connection. The victim sends the frame to the high speed connection, which was actually not the case. Therefore, malicious node extracts the desired information.

In this paper, the 'UDP' protocol and the 'ICMP' protocol were described. This old report has found that more attacks are due to these protocols. It has also been written by the author that 'DNS' is used by a lot of people, while going to Facebook or Whatsapp. The Paper has considered the mechanism of coordination between the machines involved in the attack. In case the capacity or capability of the victim is less than the volume of the data, the victim is unable to process the hidden data & the purpose of communication using covert channel is useless. It is necessary that there is an existing mechanism that will enable the victim to control the throughput of the data because the victim wants to maximize the covert communication flow. Additionally, this paper manifests the existence of the covert channels [8].

This paper contributed to the study of both components (group key management and group membership management) of the different SGC schemes by discussing their performance and efficiency according to several

criteria, namely, storage requirements, communication cost, computation cost, network model, the used cryptography type and the key update frequency [9].

This paper aims to study an Internet-based tool which can run the scans to check vulnerabilities in the system and transport the configuration files of the system [10]. This tool has the capability to scrutinize all the possibilities for locating an attacker on the Internet.

IV. Problem Definition

Denial of service (DoS) attacks are defined as attacks that are initiated deliberately in order to incapacitate the network or a machine thereby making it inaccessible for use by legitimate users[11].On the other hand distributed denial of service (DDoS) attacks are those attacks wherein an assailant tracks all the systems in the network one by one & exploits the vulnerability in one of the computer systems & then using the compromised system called the DDoS master launches further attacks within the system [12]. In existing work, the DDoS was an attempt of the attacker to exhaust the resources in the networks. This attack has been performed on more than one machine, which is also called as Botnet. The botnet is an online mode of attack that affects thousands of machines in a few minutes.

V. Objectives

1. To analyze DDoS attack in Wireless Mesh Networks

2. To propose a methodology with deploying covert channel method.

3. To implement & validate proposed technique & isolate DDoS attack.

4. To implement the proposed technique in OSPF.

5. To compare &analyze the performance in terms of throughput & delay with the proposed & existing systems.

VI. Proposed Solution

This research paper aims to provide detection and mitigation technique to prevent DDoS attacks. In this paper, we will be working on MAC (Media Access Control) address and covert channel technique. The covert channel is

ready to send maximum data towards any destination machine and we need to identify the data, whether the data has been received by the target machine. Now, MAC address stores the MAC related information into Content addressable Memory (CAM). The CAM value identifies the covert channel data and as per the proposed rule allows or denies the request accordingly. Furthermore, we propose a framework that intercepts all ARP requests and responses on untrusted ports and drops invalid ones [13].

The proposal's aim is to identify the traffic, HTTP, FTP in the upcoming technologies like IoT, cloud computing and cyber physical systems. In this exploration proposition, we will actualize the IDS structure which will shield the assault on the inward frameworks. This research proposal will be exceptionally valuable from the business point of view on the grounds that each association needs better framework to safeguard against mysterious clients. We will actualize **Switch port Analyzer** in the inner systems of the Switching Mechanism, with the simplicity to execute Intrusion Detection System. The behavior of the **IDS system** is "offline" and it generates the report to the user profound to the examination of the remote system. At the point when any irregularity is recognized on the framework then it cautions and sends a ready flag to the Gateway. The Gateway disconnects and terminates the connection of the malicious device.

VII. Proposed Methodology

Following steps will be applicable in our proposed methodology in order to mitigate DDoS attacks (Figure 3).

The first step of Segmentation: As the name suggests, it involves segmenting the network in order to either slow down or altogether prevent the threat by involving limiting the sprawl of threat to already affected areas of the network.

The second step of Inoculation: The second phase of inoculation moves collaterally in order to patch all uninfected systems with the suitable vendor patch.

The third step of Quarantine: This phase disconnects, blocks or removes the compromised devices from the network by tracking & identifying them.

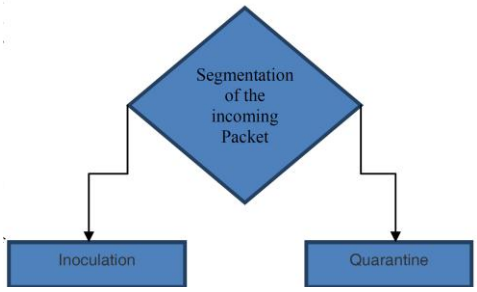

Figure 3. Mitigation of Attack.

The proposed work throws light on two segments viz detection of selfish node & mitigation of selfish node to detect & mitigate DDos attack .The proposed solution has been implemented in OSPF to ensure safety from DDOs attack in WMN.

(A) Selfish Node Detection System

Selfish node aims to save its resources to the maximum. This type of misbehaving node discards all incoming packets (control and data) .By dropping control packets, the nodes would not be included in the routing and not be requested to forward data packets. Our aim is to find out the selfish node by calculating the incoming and receiving packets. If the packets drop ratio was more and PDR (Packet Delivery Ratio) degrades by 50% then there

will be a selfish node. We also use AODV approach in this proposed work by modifying the Algorithm and detecting the selfish node.

(1) **Incomplete Audit Data:** It means data was incomplete when the topology of the network was changed and we are able to find the selfish nodes if the data was incomplete.

(2) **Find intruders by monitoring the network traffic:** By finding the intruder by monitoring network traffic we can watch the whole scenario by running the NS2 simulator and check the network summary & after that calculate the incoming and outgoing packets.

(3) **Creation of per flow:** It means that when a selfish node was created in the scenario then per flow packet movement was more and we easily find the selfish node.

(4) **Design an adaptive learning of intrusion:** An adaptive learning means that a system has to design a host based or a network based Intrusion detection system.

(B) Proposed Model

The topology (in Figure 4) used in the wireless network system contains n number of nodes i.e. $n = \{n_1, n_2 \ldots n_n\}$. In this topology Base Station Bs is a Gateway that takes the decision on the basis of command issued by the Intrusion Detection System (IDS). The IDS system accepts the packets $P[n]$ from the unknown network $\ominus$. The complete topology is modeled as linear time variant based model and any delay in the input is reflected at the output. If the delay is more than the IDS system takes time to retain the information of the System n_n. In the proposed System, the IDS system accepts the n number of packets which may be TCP, UDP or Application Layer protocols. These packets have to be processed by the IDS system, $P[n]$ and generate the output ¥.

$$¥ = P[n] * P[n] \tag{1}$$

Let us assume the dummy value k that replaces the value n then we rewrite the equation 1, as:

$$¥ = P[k] * P[k]. \tag{2}$$

If we regenerate the actual value of the signals then we follow the Time Reversal operation on packet $P[k]$ and then we get the new signal i.e. $P[-k]$. The product of the equation 2, represented in Laplace Transformation is given as:

$$P(n) = \sum_{k=-\infty}^{\infty} P[k] * P[n-k]. \tag{3}$$

This signal generated by time shifting the integer n, $P[n-k]$ and the value of the packet $P[k]$ depends on the value of $n = -1$. The output of the $P[n-k]$ has been found from Time Shifting operation of the value $P[-k]$. The desired output is $P[-k+n]$ and we get the actual result from the equation 3. In this operation the IDS identified the malicious packets and gave the information to the Base Station Bs. Now we get the output value ¥, this output value stores the information to the Server and a copy of the same file is kept by Gateway itself. We have the value of $n = -1$ which means the value of n is less than zero $(n < 0)$ and if we multiply the packet during processing then the value remains zero in each case. This means the packet is identified in exact time duration with no delay at all. This is to be considered by our proposed System and the packet has to be marked as safe. If the value goes to 1 when the value of n is greater than or equal to 1, $(n \geq 0)$, the modified equation in our case is:

$$P[n] = \begin{cases} 0, & n < 0 \\ 1, & n \geq 0. \end{cases} \tag{4}$$

The proposed model is updated based on the external inputs received by IDS system. The communication between nodes, gateway and IDS system can be subjected to Distributed Denial of Service (DDoS) attack. In this paper, we identified DOS attack, wherein the attacker compromised the system and accessed the information. Secondly, we identified the scenario wherein the attacker compromised two or more internal nodes and then these infected nodes spread malicious data to the entire network system. To address these problems, we made a mathematical System that was also implemented in network simulator and we also evaluated the performance results.

(C) Proposed Algorithm

In this section, the proposed Algorithm has been divided into two processes, initial process and Assign process. In the initial process, the gateway is connected to the external network and it receives the incoming request from the outer network to route the data from source to the destination. The basic information of the outer node like IP Address and MAC Address is then stored in the routing table.

Initial Process ()

1. Outer network sends HELLO message to the Gateway for establishing connection.

2. Gateway builds the neighbor Table 'Routing Table' and stores the information related to the unidentified node.

Assign Process ()

1. IDS node identified the packet $P[k]$ which is received by the Gateway.

2. If IDS found malicious or dummy packets then it blocks the packets and informs the Gateway.

3. The Gateway discards the connection and store its MAC value to the MAC Address Table which is used for future purpose.

4. If outer node broadcasts the HELLO message and bypasses the connection then IDS itself blocks the connection. This happens due to timeslot and hop based model:

$$\min(n,\ k+1+\cdots+(k+1)^H).$$

In the Assign Process, the IDS device receives the packets and these packets are processed by the Gateway. Now, the Gateway makes two Pool tables, In the First pool, it stores the information of normal node and in the second pool table it saves the information of abnormal nodes that create malfunctioning. If the repeated abnormal node creates malfunctioning, then the Gateway itself discards the connection and that activity is reported to the IDS system. This process can save a lot of time because we investigate that IDS takes some time to process any activity (Figure 5).

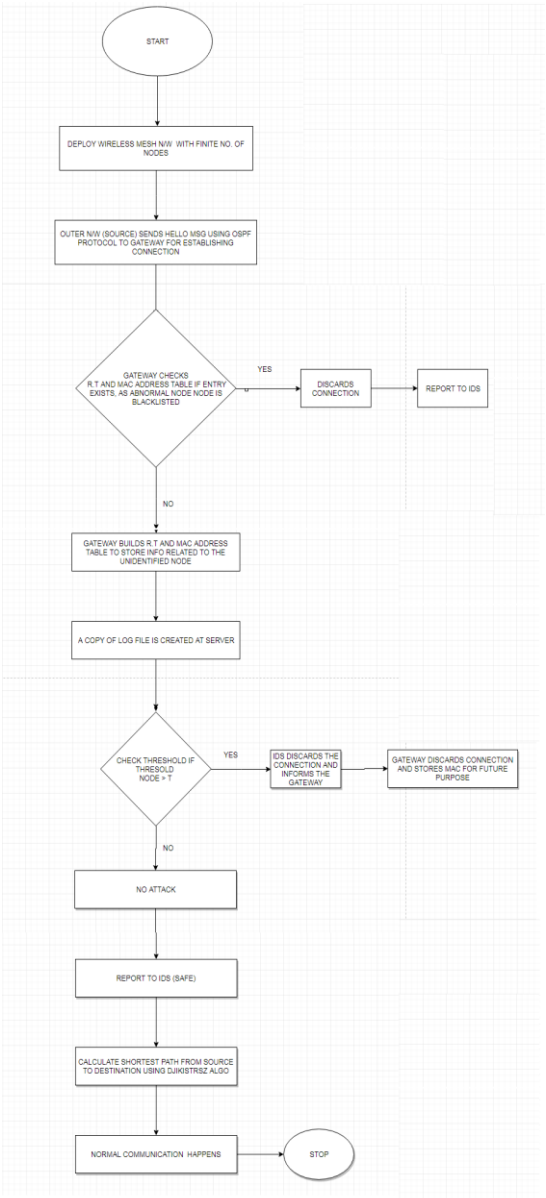

Figure 5. Flowchart of proposed work.

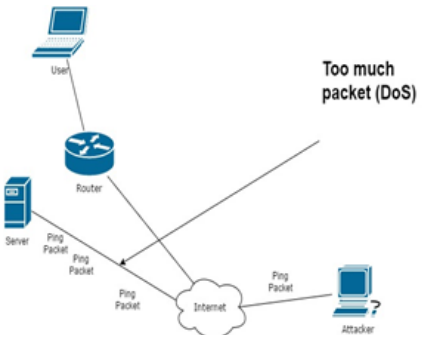

Figure 4. Denial of Service Attack.

VIII. Simulation Results

We will take the same threshold value to detect the attack i.e.; 1200 mAhr [2]. If the threshold value of a node is more than the said threshold value that means attack has been performed in the network. We were getting the MAC address from the malicious node that performed such kind of activity and this node's address would be blacklisted. In our topology 3 & 18 are the malicious nodes.

If the same node i.e. malicious node will be communicating in future then the node will be blocked by the base Station node. The base Station had stored information related to this node into the log file. This log information was shared with the gateway as well as the network administrator. We are using some important protocols which are being implementing in the proposed scenario: (Figure 6)

1. Dynamic source routing protocol is used in the proposed scenario that calculates the shortest path before the node is deployed in the network.

2. Route initialization information is stored in the cache memory.

3. Shortest route calculation depends on weight and hop count.

4. In our case, the route initialization and shortest path determination is based on hop count and distance.

Table 1. Simulation Statistics.

Parameter Used	Value
Number of Nodes	30
Nodes Speed	10 m/s
Sender	10
Receiver	20
Movement	Random Waypoint Model
Area	1000m * 1000m
Protocol	AODV, OSPF
Data Rate	24 Mbps
Simulation Time	100s
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11 MAC Layer
Antenna Type	Omni directional
Packet Size	1024 (bytes)
Malicious Nodes	3, 18

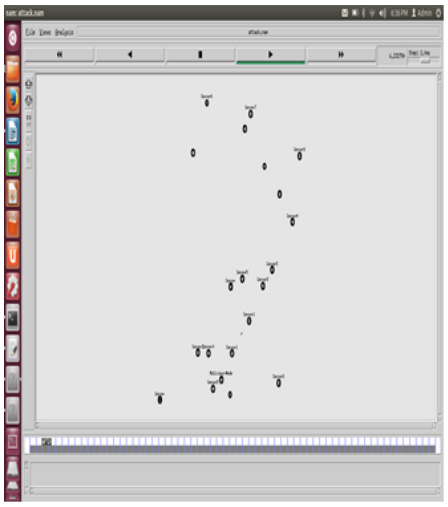

Figure 6. Implemented Model in NS-2.

In the second case (see figure 7), the proposed system was developed to

rectify the DDoS attack and battery charge down from the initial charge process is 0.1 %. This is the way we can achieve the process. The major difference between initial process and normal process is about 99.3%. If we consider the case of proposed and normal case then it is 99.8%. Also difference between initial and proposed method is 99.13%.

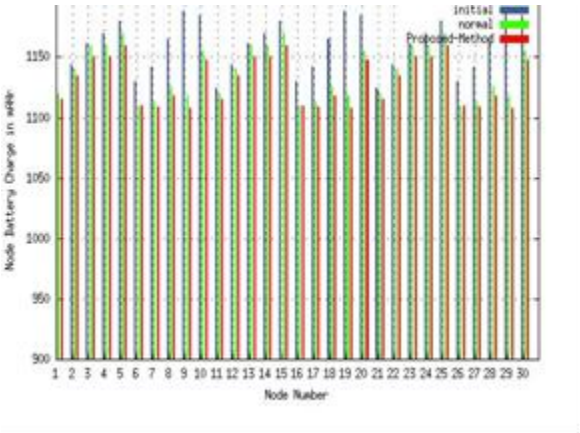

Figure 7. Node Battery Charge.

(A) Throughput: Figure 8 shows the throughput of data transmission. on the basis of route discovery process and computation of the feasible path that satisfies the Quality of Service (QoS) constraints. This is also due to the mathematical equation, explained in section VII.-A. It is also seen that when applying the security mechanism in the network topology, overhead of the system increases exponentially and reduces the cost of throughput. However, the proposed system implements pool based system and thus reduces the overall delay of the system. In fact, it eliminates the looping concept. As a result, the throughput is higher in our case i.e. 78 Mbps.

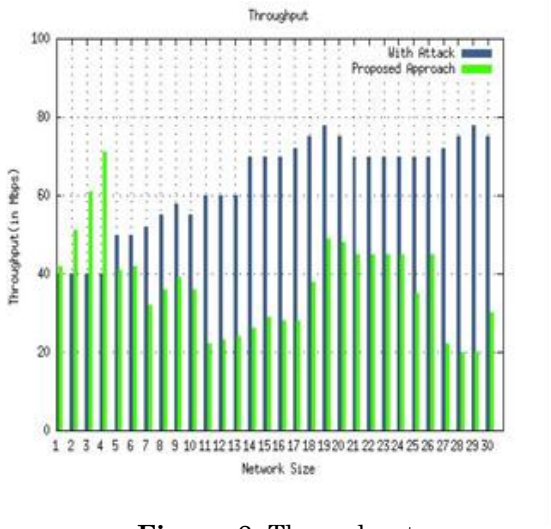

Figure 8. Throughput.

(B) End to end delay: It can be noticed in the Figure 9 that delay reduces for all nodes when the communication takes place. This reduction is achieved because the IDS gives the feasible route to the packet from the source node to the destination node. The delay in the existing network goes higher because the $P[n-k]$ reaches the value 1, the node selects the malicious path and the information might be accessed by the intermediate node. However, the proposed Algorithm along with IDS provides effective route to the node from source to the destination.

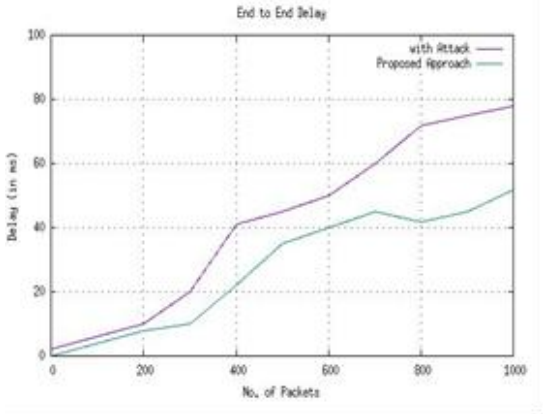

Figure 9. End-end delay.

IX. Conclusion

This paper aims to analyze DDoS attack and propose a framework for mitigating the same. This will help to protect the Internet applications and API's from malicious traffic targeting network and allow the application layer to maintain availability and performance through proposal of proper mitigation technique for containing DDoS attacks after detection. In order to make WMNs security aware this paper proposes a technique for the detection & mitigation of DDOs in WMNs. The paper applies the proposed methodology in OSPF. Malicious nodes are identified by the IDS as well as the PDR calculation. The IDS then generates the offline report to the user after the examination of the remote system. If any malicious activity is found gateway is informed which then blocks the user. Furthermore the node is blacklisted; Mac address of the abnormal node is stored in CAM to safeguard the network against future attacks. It has also been observed that the attacking technique has a large impact on AODV than OSPF.OSPF is better in terms of performance than AODV. This paper also evaluates the effect on the throughput and end-to-end delay of the network after attack. This paper also analyzes the result after the application of proposed solution for mitigation of the attack in the network.

References

[1] Aggeliki Sgora, Dimitrios D. Vergados and Periklis Chatzimisios, A Survey on Security and privacy issues by Wireless Mesh Networks, 2016.

[2] E. Cedex, Protecting Wireless Mesh Networks through a Distributed Intrusion Prevention Framework (2015), 1-6.

[3] H. Al-Mefleh and O. Al-Kofahi, Taking advantage of jamming in wireless networks: A survey, Comput. Networks 99 (2016), 99-124.

[4] Y. Yu, Z. Ning, Q. Song, L. Guo and H. Liu, A Dynamic Cooperative Monitor Node Selection Algorithm in Wireless Mesh Networks, 2015.

[5] T. Sommestad and F. Sandström, Information Computer.

[6] Security & quot; Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study & quot; An empirical test of the accuracy of an attack graph analysis tool, Anal. tool Inf. Comput. Secur. Comput. Secur. Iss Inf. Comput. Secur. 23(5) (2015), 516-531.

[7] Z. A. Baig and A. I. Khan, DDoS Attack Modeling and Detection in Wireless Sensor Networks, Mob. Intell. (2010), 595-626.

[8] D. Kaur and P. Singh, Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack, 5(1) (2014).

[9] M. Mehic, J. Slachta and M. Voznak, Whispering through DDoS attack, Perspect. Sci. 7 (2016), 95-100.

[10] O. Cheikhrouhou, Secure Group Communication in Wireless Sensor Networks: A survey, J. Netw. Comput. Appl. 61 (2016), 115-132.

[11] M. Ahmed, A. N. Mahmood and J. Hu, A survey of network anomaly detection techniques, J. Netw. Comput. Appl. 60 (2016), 19-31.

[12] E. Technique and F. Preventing, Enhanced Technique For Preventing and Isolating Distributed Denial of Service Attack in Wireless Mesh Networks, pp. 1-38.

[13] S. Behal and K. Kumar, Trends in Validation of DDoS Research, Procedia Comput. Sci., 85 (2016), 7-15.

[14] I. Almomani, Performance Analysis of LEACH protocol under Denial of Service Attacks, (2015), 292-297.