International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8, Issue-9S, July 2019

Preventing & Isolating Distributed Denial of Service (DDOS) attack in Wireless Mesh Networks (WMN's)

Afshan Hassan, Rajeev Sharma, Gurbaj Singh

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 authors have tried to present their work on first detecting it and later on fixing it. With the help of different protocols present in the Application Layer, a hacker takes information out of the script. The authors have used Covert Channel, which has been mentioned in many essays. Now with the help of this channel, the information will go to all and it will not go to any of the informatics. This research proposal envisions a methodology to first detect the selfish node in the network & later on provides a technique for mitigation of the same.NS2 simulator has been used to simulate & analyze the performance of our proposed methodology for Open Shortest Path First (OSPF) protocol in WMN's.

Index Terms—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)

I. INTRODUCTION

Wireless Mesh Networks (WMN's) consist of Wireless Access points (AP), Mesh routers (MR's) & 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].

Revised Manuscript Received on June 15, 2019.

Afshan Hassan, Rajeev Sharma, Gurbaj Singh, CEC Landran, India

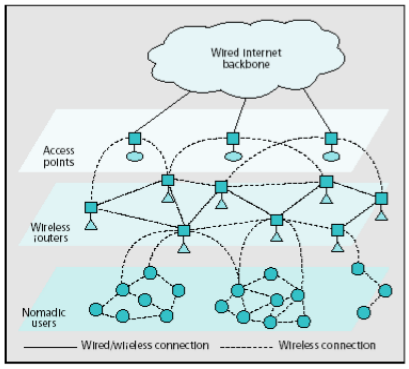

Fig. 1.: Architecture of wireless mesh network

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]. 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, design issues & security threats 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 & simulation results are discussed in Section VII &Section VIII.

II. CHARACTERISTICS, DESIGN ISSUES & SECURITY THREATS IN WMNS

A. Characteristics of Wireless Mesh Networks:

1) *Self organization & 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. Design issues in WMN's [2][3]

1) *Energy Consumption:* Nodes in a mesh network are battery dependent. Mesh nodes are placed in hostile environments so replacing the battery is quite impractical. Hence energy conservation and management is a challenging task to resolve in a wireless Mesh network.

2) *Fault tolerance and adaptability:* Fault tolerance is the ability of a mesh network to maintain different functionalities of the network without any interruption in the event of failure of Mesh nodes. When any node fails,an adaptive protocol adjusts it to generate new link.

3) *Scalable and flexible architecture:* In a Mesh network, the number of Mesh nodes deployed may be of the order of hundreds, thousands or millions so that we can easily extend the network size. The communication protocols must be designed in a way that all the deploying nodes in the network do not affect clustering and routing. In other words, the network must preserve its stability.

4) *Error-prone wireless medium:* Mesh networks can be deployed in different situations and the requirement of each application is also different. Wireless medium can be greatly affected by noisy environments. An attacker causes noise to affect the communication and create interference

5) *Synchronization:* Clock synchronization is an important service in Mesh networks. Time Synchronization in a Mesh network aims to provide a common timescale for local clocks of nodes in the network. A global clock in a Mesh system will help analyze the data correctly and predict future system behavior. Some applications that require global clock synchronization are environment monitoring, navigation guidance, vehicle tracking etc. A clock synchronization service for a Mesh network has to meet challenges that are substantially different from those in infrastructure based networks .

6) *Node Deployment:* Mesh networks can be deployed randomly in geographical areas. Without human intervention they can be maintained automatically. In a Mesh network, node deployment falls into two categories __a dense deployment & a sparse deployment. In dense deployment the targeted field contains high numbers of Mesh nodes. While in a sparse deployment we have fewer nodes. Dense deployment is used to detect multiple meshes. Whenever cost of production increases it can be used there.

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.

1) Security and Privacy Requirements

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

2) 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.

3) 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.

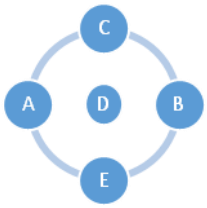

Fig. 2.: Message Integrity of Mesh Networks

4) 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

This paper discusses an efficient real time predicate based traffic approximation dependent denial of service detection model. The network trace has been taken as input & splitted into a number of time windows. Each subset of traces belongs to a different time window. Different features have been extracted. With the extracted features, different average values on payload, hop count, latency have been measured. Similarly using the malicious trace, the method estimates the various features. Using all the features extracted, the method generates the predicate closure for different services in each time window. For classification purpose, the method computes the predicate closure weight. Using the predicate closure weight estimated for the incoming packet the method performs classification of the packet [7].

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 [8].

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[9]. This tool has the capability to scrutinize all the possibilities for locating an attacker on the Internet.

This paper proposed a solution for the detection & prevention of DDoS attacks in WSNs for AODV protocol & DSR protocol using energy analysis technique. Different network parameters viz Throughput, delay etc. were studied before & after the DDoS attack in the network. It was observed that attacking technique has large impact on AODV than DSR routing protocols. Proposed solution enabled longer network life because malicious nodes were shut down once detected [10].

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.[11]

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[12].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 [13]. 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 SOLUITION

This research paper aims to provide a detection & mitigation technique to prevent DDoS attacks. In this paper, we will be working on MAC (Media Access Control) address and covert channel technique. MAC address stores the MAC related information into Content addressable Memory (CAM).

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. We will actualize **Switch port Analyzer** in the proposed research proposal to execute Intrusion Detection System. Whenever any irregularity is recognized on the framework, IDS cautions and sends a ready flag to the Gateway. The Gateway disconnects and terminates the connection of the malicious device. IDS also generates an offline report of the system to the user after the examination of the system[13]

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 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 the 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.

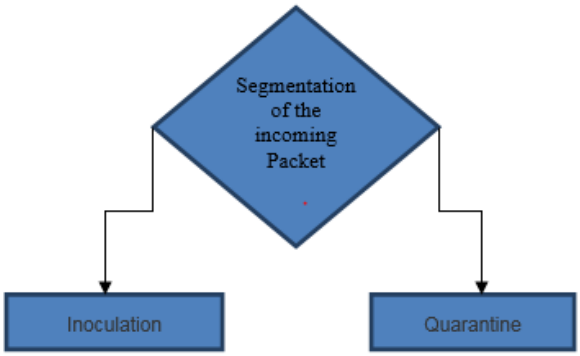

Fig. 3: Mitigation of Attack

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 the 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 received packets. If the packet 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.

a) *Incomplete Audit Data:* It means the 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.

b) *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.

c) *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.

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

B. Proposed Model

The topology (Figure 4) used in the wireless network system contains n number of nodes i.e. $n=\{n_1,n_2\text{----}n_n\}$.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 ɵ. 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 then 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 other Application Layer protocols. These packets have to be processed by the IDS system, P[n] and generate the output ¥.

¥= P[n] * P[n] ---------- (1)

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

¥= P[k] * P[k] ---------- (2)

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

$$P(n) = \sum_{k=-\infty}^{\infty} P \text{-------- (3)}$$

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≥0), the modified equation in our case is:

$$P[n]= \begin{cases} 0 \\ 1 \end{cases} \text{---------- (4)}$$

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.

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:

$$\min(\, n, k+1+\ldots\ldots\ldots\ldots+(k+1)^{H})$$

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. (Figure 5).

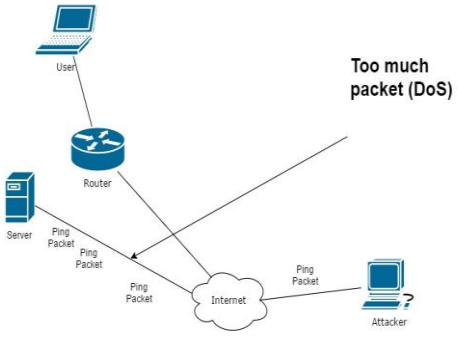

Fig. 4.: Denial of Service Attack

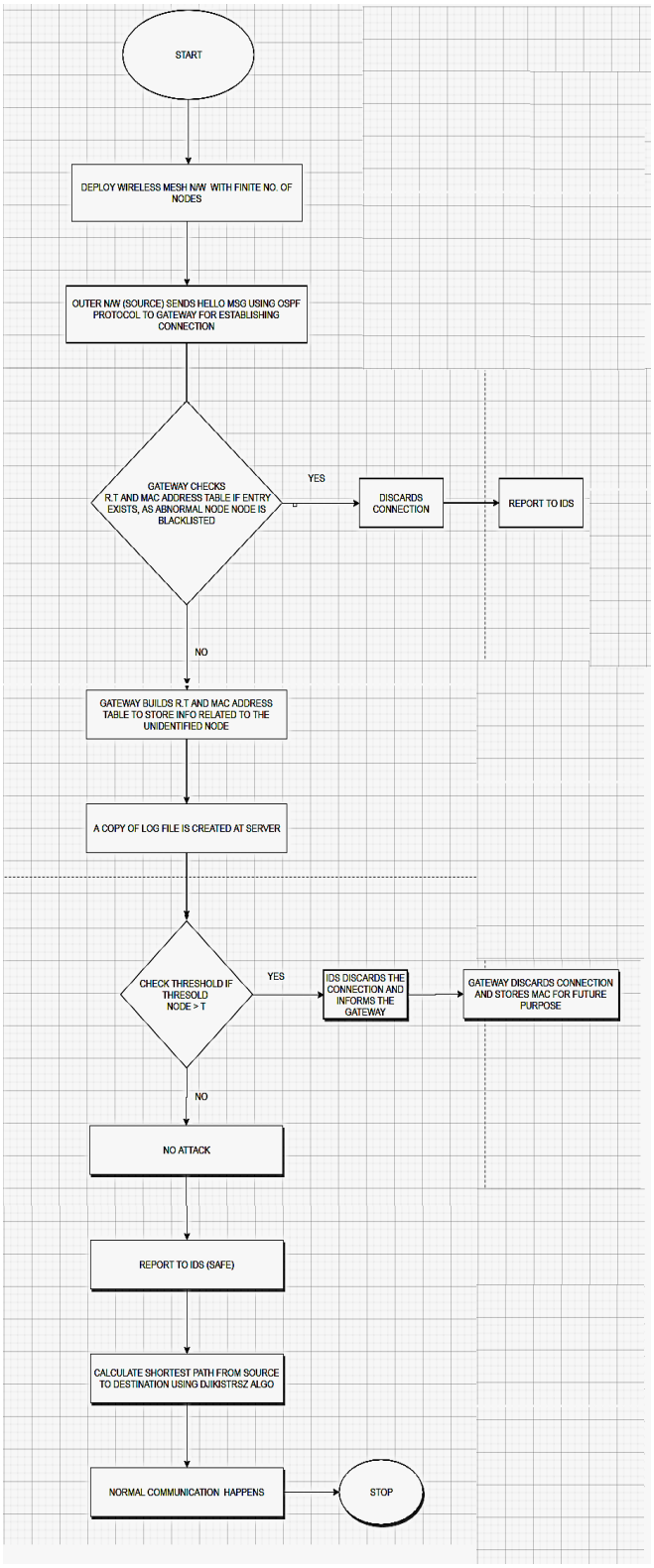

Fig. 5.: Flowchart of proposed work

VIII. Solution Implementation, Results & Discussions

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.

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

We conduct the simulations on the network recreations and execute the proposed algorithm to explore the results. The input values given to the OTCL script are given in table 1. The entire experiment is executed on the IEEE 802.11, this standard alludes to the Wireless Mesh Networks (WMNs). The radio range is kept the same [1], 15m with a distance of range 10m to 12 m, as indicated regarding the movement of the node. We have used OSPF protocol that calculated the shortest path from the running nodes .The constant bit rate (CBR) calculates the execution time of packet IN and Packet OUT.

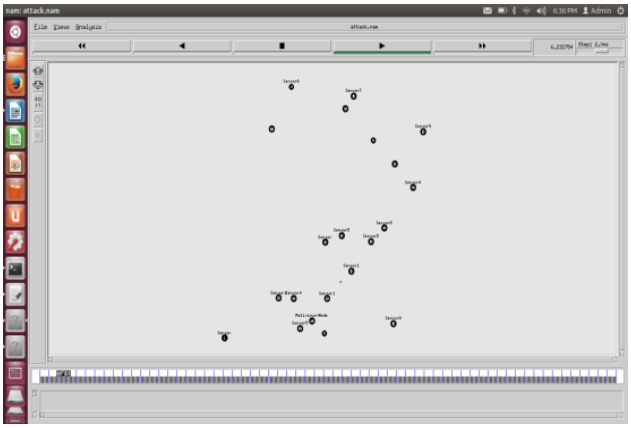

Fig. 6.: Implemented Model in NS-2

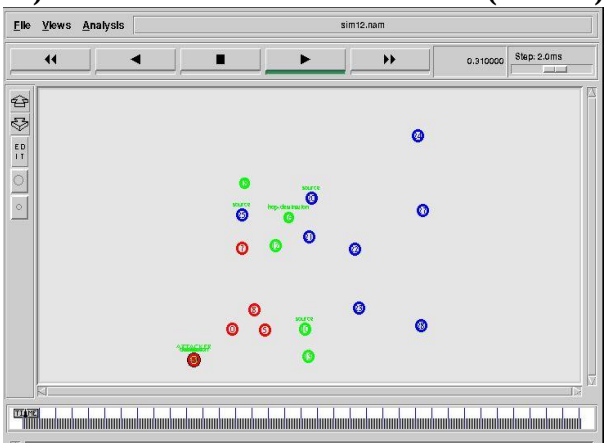

Fig 7: Nodes adjusted their positions

We input the time so that the source node sends the data to the hop node in timely manner. The two nodes, source node and destination node are physically located because we display in the simulated scenario, how the simulation is performed. Also the integration of Adhoc nodes is displayed.

A. Transmission range of Adhoc Nodes:

Figure 8 exposes the transmission range between the Adhoc to Adhoc node and cluster to cluster node. The cluster concept has some unique features that were not in Adhoc node. Clustering is the process wherein the whole network is divided into clusters. Every node in a cluster elects a base node or leader, which is also known as cluster head. In our case we are using observer that observes every movement of the Adhoc node. In the meantime, transmission range shows how many nodes come in single node range. Every single node range identifies the neighbor node with the help of transmission range.

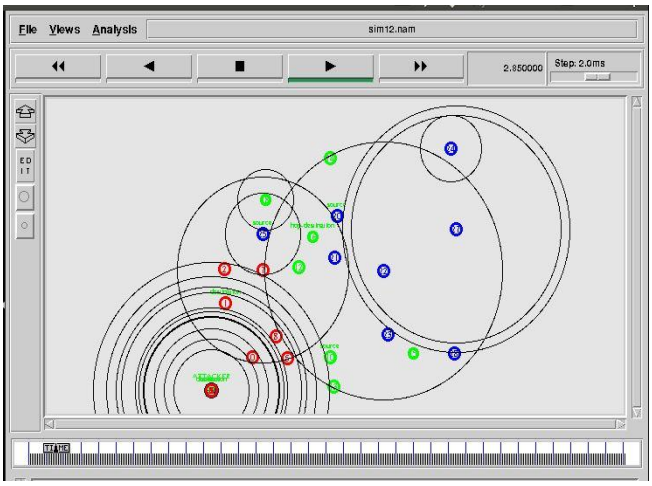

Fig. 8.: Transmission range of Adhoc Nodes

B. Activation of attacker node

Figure 9 depicts attacker node activation in the Mesh Network area. The attacker node senses the entire area using Service Set Identifier (SSID). SSID is a unique feature in the wireless network that senses the position of wireless node by using beacon messages. The attacker node continuously sends beacon signals to different

nodes present in the network. Now, the attacker node tries to enter the network using different methods and if the node enters in the workspace then it disrupts the whole traffic and accesses important information.

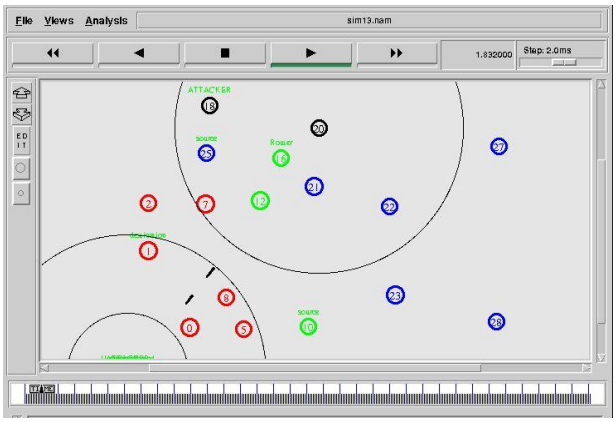

Fig. 9.: Attacker Node Activation

C. Battery Charge

During the initiation process of DDoS attack, the adversary compromises vulnerable nodes in the network and installs the source code that is in the form of script. The code is written in such a way that it awaits to trigger the call. The moment the code is executed it immediately lowers down the battery charge.

Battery Charge = Power*Time ------- (1)

Power is in watts and time is in seconds

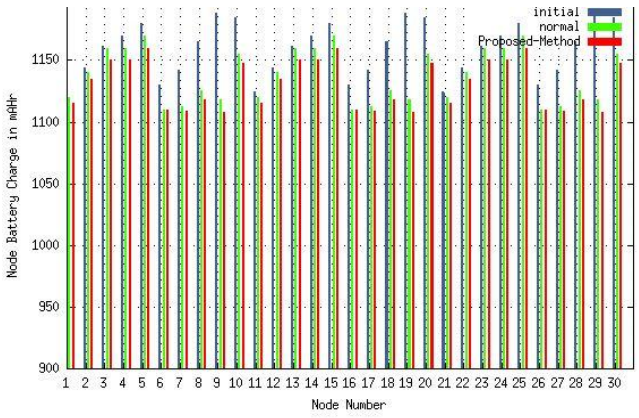

Fig. 10.: Node Battery Charge

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 proposed and normal case then it is 99.8%.Also difference between initial and proposed method is 99.13%.(Figure 10).

IX. CONCLUSION

This paper aims to analyze DDoS attack & proposes a framework for mitigating the same. This will help to protect the Internet applications & API's from malicious traffic targeting network & allow the application layer to maintain availability & 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 proposed algorithm does not send out extra control packets in the networking to route packets. There is no need to watch all neighbors' behavior. Only the next hop in the routing path should be observed. As a result, the system performance wastage on detection algorithm is lowered. Distributed anomaly based IDS system is more complex as it requires cross layer interaction to detect an attack and its distributed nature can have more threat points in the network 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.

REFRENCES

1. Ali Mahmodi, Parisa Daneshjoo, Changez Delara,"Using Genetic Algorithm to Improve Bernoulli Naïve Bayes Algorithm in Order to Detect DDoS Attacks in Cloud Computing Platform"2018
2. E. Cedex, "Protecting Wireless Mesh Networks through a Distributed Intrusion Prevention Framework," , 2015, pp. 1–6.
3. H. Al-Mefleh and O. Al-Kofahi, "Taking advantage of jamming in wireless networks: A survey," Computer Networks, vol. 99, 2016, pp. 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"2014
6. Security & quot; Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: An empirical test of the accuracy of an attack graph analysis tool," Inf. Computer. Security, vol. 23, no. 5, 2015, pp. 516–531.
7. M.Baskar,T.Gnansekaran,J.Frank Vijay: Time Variant Predicate Based Traffic Approximation Algorithm for Efficient low Rate DDoS Attack TAGA Journal,2018 ,Vol 14
8. M. Mehic, J. Slachta, and M. Voznak, "Whispering through DDoS attack," Perspect. Sci., vol. 7, 2016, pp. 95–100.
9. O. Cheikhrouhou, "Secure Group Communication in Wireless Sensor Networks: A survey," J. Network. Computing. Appl., vol. 61, 2016, pp. 115–132.
10. R. Upadhyay, Salman Khan,Herendra Tripathi,Uma Rathore Bhatt"Conference on Computing and Network Communications(CoCONet'15)",2015

11. D. Kaur and P. Singh, "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack," vol. 5, 2014, no. 1.
12. M. Ahmed, A. N. Mahmood, and J. Hu, "Journal of Network and Computer Applications A survey of network anomaly detection techniques," J. Network. Computing. Appl., vol. 60, 2016, pp. 19–31.
13. E. Technique and F. Preventing, "Enhanced Technique For Preventing and Isolating Distributed Denial of Service Attack in Wireless Mesh Networks," pp. 1–38.

AUTHORS PROFILE

A young & talented research scholar who has dedicated her whole life for the betterment of society. Pursued B.tech & presently pursuing M.tech(last semester) from CGC Landran.I have attended conferences & have published three papers so far.I am a certified Cisco trainer & have worked as an Assistant Professor for a period of 6 months at SSM college of engineering & also worked for one year as a Cisco trainer

I am presently working as an Assistant Professor at CGC, Landran. I have completed my B.Tech & M.Tech(CSE) & I am currently pursuing PHD from Chandigarh university. I have published 15 research papers & have 11 years of experience in teaching.

I am presently working as an Assistant Professor in computer science and engineering department. I have completed my B.Tech & M.Tech(CSE) I have published many research papers & have more than five years of experience in teaching.