RESEARCH ARTICLE OPEN ACCESS

Distributed Denial of Service Attack Detection, Prevention and Secure Communication in MANET

Ranjana Kumari [1], Achint Chugh [2]

Department of ECE
MIT, RGPV, Bhopal
M.P – India

ABSTRACT

Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such network changes expeditiously. To accomplish availability and reliability network routing protocols should be prevailing compared to distributed type of denial of service security attacks. Distributive denial of service (DDoS) makes the network resources unavailable. In DDoS attacks the incoming traffic flooding the nodes from many different sources. Determination of data link letdown, info safety, recognition of malicious node and protected information transmission within MANET is a significant tasks in any mobile network. This paper proposed a DDoS attack detection and prevention scheme. The proposed algorithm detects the possibilities of DDoS attacks in the network and prevents the network, provide security.

Keywords:- MANET, AODV, Routing, Node Security, DDoS, LDDoS

I. INTRODUCTION

The growth of mobile devices and 802.11 Wi-Fi wireless networks security is on demand topic of research in MANET[1]. Ad-hoc network doesn't depend on any stable infrastructure or central administration such as base. Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such network changes expeditiously. The brilliance of service essentially satisfy source end to destination end data packet transfer without packet loss. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared.

To accomplish availability and reliability[2] network routing protocols should be prevailing compared to distributed type of denial of service security attacks. The credibility of allocating data packets from end to end using more than one intermediary hopes is a remarkable problematic in the mobile Adhoc network. Because to the innately self-motivated nature of the mobile system network layout, the prevailing data routes cannot be secure. Determination of data link letdown, info safety, recognition of malicious node and protected information transmission within MANET is a significant tasks in any mobile network.

As per the style of operation ad-hoc network are basically works on peer to peer communication among many node mobile wireless network[4]. Most of the uses of MANET are: Military drill or police routine, Disaster relief operations, Mine site operations, Urgent meetings, Robot data acquirement, Packet radio network, Commercial application like third generation network. MANET's having number of node demands high quality of processing power, high bandwidth, security[3] and memory to provide definite routing information, though induces traffic overhead in the network. In this the information of data are circulates in the network. MANET has some boundaries in arrears to capabilities of mobile nodes, infrastructure, mobility, or because of system as a whole. Limitations due to infrastructure or system, Variable capacity links, Broadcast method of communications, Frequent partitions/ disconnections , Packet loss due to transmission error, and limited bandwidth. As when nodes communicate to each other for transferring the information consumes more battery power in return. The thought of Ad-hoc networking usually termed as infrastructure less networking. In this type of the network, mobile devices functions as router and as host. They forward the information packet to other devices even if they are not in direct range of transmission. Limitations due to mobility, Dynamically changing topologies, Lack of mobility awareness by system/applications, Tedious identification mechanism / IP address assignment, Limitations due to capabilities of mobile nodes, Short battery life. Limited capacities – memory, radio range, application softwares.

A DoS[5] attack prevents users from accessing the services. In DoS attack node sends excessive messages to block the services. Distributive denial of service (DDoS)[5] makes the network resources unavailable. In DDoS attacks the incoming traffic flooding the nodes from many different sources.

DoS attacks usually flood networks, or systems massive traffic in order to overthrow the target resources and make impossible or difficult for valid users to use services. DoS attacks are more difficult to recover, identify or prevent. The DoS attacks almost crashes the node and blocks most of the path of the network. DOS attacks degrades the network performance and drop the packet delivery ratio. The prevention and detection of DoS attack in a network is challenging task for the researchers. The network used firewalls, intrusion prevention system and intrusion detection systems for DoS attack prevention and detection. DDoS attacks are basically from more than one attack systems. DoS attacks are easy to detect from DDoS because simple DoS attack is originated from single node while DDoS attacks are originated from multiple systems. DDoS attacks shut down the services of network, application or system and flood the target with traffic and disturb the network. DDoS attacks shut down the services of network, application or system and flood the target with traffic and disturb the network. Although DoS attacks do not usually result in the loss or theft of noteworthy information or other resources, they can cost the target a countless treaty of money and time to handle. DoS attacks can crashing the services or flooding the services. Flood attacks take place when the network system accepts ample of traffic for the server to buffer, triggering them to sluggish down and ultimately stop the services. The flood DoS attacks are ICMP flood, buffer overflow and SYN flood.

ICMP flood – influences misconfigured network components by directing bluffed packets that ping every single computer on the under attack network, in its place of just one definite machine. The network is then generated to strengthen the traffic. This type of attack is also known as the ping of death or smurf attack.

Buffer overflow attacks – is the most common DoS attack. The notion is to direct additional traffic to a network node than the node have built the system to handle.

SYN flood – it sends a demand to connect to a server, but not once finalizes the handshake signal. Remains up until all exposed ports are drenched with demands and no one are obtainable for authentic users to connect to.

The important dissimilarity is that in its place of actuality attacked from single place, the target node is criticized from numerous places at once.

The locality of the attack is problematic to identify because of the arbitrary delivery of attacking systems. The factual attacking node is more problematic to recognize, as they are disguised behind numerous or typically compromised nodes. It can influence the larger volume of nodes to implement an extremely disrupting attack. It is further problematic to shut down numerous nodes than one.

The objectives are to detect distributed denial of service attack in MANET, to provide prevention of MANET from distributed denial of service attack,

The rest of the paper is organized as follows.

Section 2 represents related work about DDoS prediction, detection and failure. Section 3 provides proposed algorithm. Section 4 provides the implementation and result analysis of proposed algorithm. Section 5 concludes the paper with a summary of the work and discussion of future research directions.

II. RELATED WORK

Yu[6] proposed a collaborative approach of protection compared to episodic shrew DDoS attacks in the low frequency domain. This methodology identified shrew DDoS attacks with the help of frequency-domain characteristics from the auto-correlation arrangement of Internet traffic data streams.

Wu[7] presented an LDoS attack detection method using the technique of one step prediction Kalman filtering. This method explored the characteristics of network traffic observed at the victim end when the attack started. The error between one step prediction and the optimal estimation is used as the basis for detection.

Preventing Malicious Node[8] and Provide Secure Routing In Manet. This paper provides SIEVE, a completely disseminated procedure to recognize malicious nodes. SIEVE is robustness and precise accurate under numerous attack situations and misleading actions. The methods implemented for the identification and the subsequent elimination of malicious nodes openly require a careful design and joint to enhance the complete performance.

An Innovative Hybrid Trust Management[9] Structure for MANETs is to design a powerful and robust trust management framework for DDoS. A hybrid trust management framework (HTMF) to build trust setting for MANETs. The limitations is it will not work on selective misbehave attack and time attacks.

Recommendation Based Trust Model[10] with an Effective Defence Scheme for MANETs provides reference constructed trust model with a protection scheme, which utilizes grouping technique to energetically filter out attacks associated to untruthful recommendations using assured time based on amount of interactions, closeness between the nodes and compatibility of information. It only detect bad mounting attack. It does not provide prevention and detection from DDoS based attacks. Extenuating the Attacks on Commendation Trust Model for Mobile Ad Hoc Networks. This[10] provides information about recommendation based trust model for MANET. It successfully provides details and differentiated the honest and dishonest recommendations. This algorithm will not work on LDDoS based attacks.

At present-day, more and more compound system network traffic is designated by using a traffic prototypical in network traffic capacity. Low-rate denial of service (LDoS)[8] cyber-attack direct periodic pulse series with comparative little rate to form combination flows at the target end. LDoS attack movements have the characteristics of great concealment and low average rate. Low-rate Denial of Service (LDoS) attack is a new type of DoS attack. LDoS attacks demonstration an episodic pulse arrangement, which can be communicated in a triple of attack epoch T, attack duration L, and attack rate R. LDoS attacks direct attack data packets from time to time in a little time interval. The system network multifractal must be interrupted when LDoS attacks are launched unexpectedly. Barford presented the wavelet handling idea in discovering LDoS attacks by using the DWT discrete wavelet transform[11] technology. This technique transforms network data traffic into middle, high, and low frequency components for the perseverance of discovering the attack traffic.It is tough to identify LDoS attack streams from standard traffic because of low data rate property. Although the LDoS attack movements are very minor, it will inescapably lead to the variation of multifractal appearances of network traffic. LDoS attacks effort to contradict bandwidth to TCP flows while conveyance at satisfactorily low average rate to get away detection by counter-DoS mechanisms. The LDoS attacks may well retain damaging the target for a lengthy period without being detected. DDoS oriented detection methods are no longer suitable for the detection of LDoS attacks. The investigators found that the self-similar prototypical with its only scaling consideration is not adequate as a manifold scaling on fine timescales.

The procedure of multifractal detrended oscillation analysis (MF-DFA)[12] is used to discover the modification in relations of multifractal features over a minor scale of network data traffic due to LDoS attacks. A novel methodology of distinguishing LDoS attacks is suggested by observing the unexpected change of Holder exponent using wavelet investigation. The DFA procedure is extensively used in authenticating the scale characteristic of monofractal and in perceiving the long-range connection of noisy nonstationary sequences. By using the MF-DFA algorithm, researchers can achieve the multifractal spectrum easily and analyze the multifractal characteristic of nonstationary sequences effectively.

III. PROPOSED WORK

The proposed work is presented in this section. The proposed algorithm and its description is give below.

The algorithm description is given in this section. In initialization phase threshold values for queue length, packet number, packet delivery ratio is initialized for parameter testing. The routing protocol is set as AODV, the number of nodes are set as 50. The maximum and minimum queue size is set maxqu is set as 85% and minqu is set as 25% of queue length. Warning is half the queue size.

The algorithm is given below.

```
Algorithm
Step 1: Initialization step: miniqu=0.25 * qusize, Maxiqu=0.75 * qusize, Warn=qusize/2
Step 2: Threshold value setup for queue size, packet delivery ratio
Routing protocol setup, Node setup, Scenario setup, Source and destination setup,

Step 3: Each node checks its congestion statues by using average queue length, Compute average queue length
    The frequency of data packet is decided according
        to congestion status
        If frequency is high then
            Ok incoming traffic is low, no DDoS attack
                in network
        Else if check packet number is increases above
            threshold value then
            LDoS attacks in the network
        Else if test packet delivery ratio of the node
            packet distribution ratio dew drop to the
            given threshold then
            DDoS occurrence is identified in the
            network
            Source node randomly choose the next
            neighbor
        If some node response from additional route
            excluding neighbor node
            Then trigger the inverse locating method
            and send data packets
            Test messages to determine Distributed
            denial of service occurrence
            Marked node list attacked node onto DDoS
            attack node list
            Activate alarm
        Goto End

    Else if frequency is low, DDoS attack in network
        Then
        Traffic is high, alternate best bath is dynamically
            established and data can be transmitted
        End if
Step 4: End
```

Each node checks its congestion statues by using average queue length. The computed average queue length is used to check DDoS attack in network. The frequency of data packet is decided according to flooding status in network. If frequency is high then network is fine incoming traffic is low, no DDoS attack identified in the network. Otherwise check packet number is increases above threshold value then LDoS attacks is identified in the network. Otherwise test packet delivery ratio of the node packet distribution ratio dew drop to the given threshold then DDoS occurrence is identified in the network. Source node randomly choose the next neighbor if some node response from additional route excluding neighbor node then trigger the inverse locating method and send data packets. Test messages to determine Distributed denial of service occurrence. Marked node list attacked node onto DDoS attack node list. Activate alarm packet and distribute in the network about DDoS attack detection. Else if frequency is low, DDoS attack in network then traffic is high, alternate best bath is dynamically established and data can be transmitted.

IV. IMPLEMENTATION

The program is developed in TCL language and some functions are also implemented in C/C++ language. For simulation environment we used i3 2.0 GHz machine with 4GB RAM. NS2 is used as simulation environment. In implementation work, network used 50 nodes, which are arbitrarily positioned in dissimilar parts of positioning part with a static density. For this implementation, network parameters, such as Dimension, Number of nodes, traffic, transmission rate, Routing protocol, transmission range, sensitivity, transmission power etc., are used.

Simulation Parameters

Simulation area	500m X 500m
Simulation duration	500 s
No. of Adhoc nodes	50
Transmission range	300 m
Movement-Model	Random-Waypoint
Traffic-type	CBR
Max. mode-speed	12 m/s
No. of connections between nodes	5 – 30
Pause time	10 s
MAC	802.11
Source Destination Pair	15
Radio Range	250 m
Rate (packet per sec)	2 pkts/s
Data pay-load	30 – 512-bytes
Seed	1.0
Protocol	AODV

Table 1: Simulation parameter

The implementation result is given in the figure below.

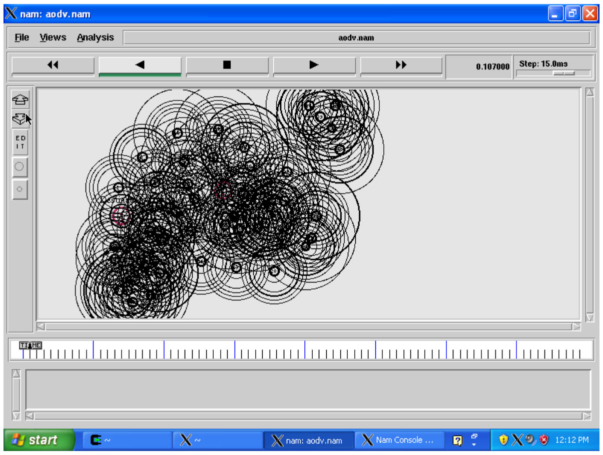

Figure 1: DDoS attack detection in network

The network with DDoS attack is given in the figure above. As DDoS increases in the network the packet drop is increased and node will not provide any services to the network.

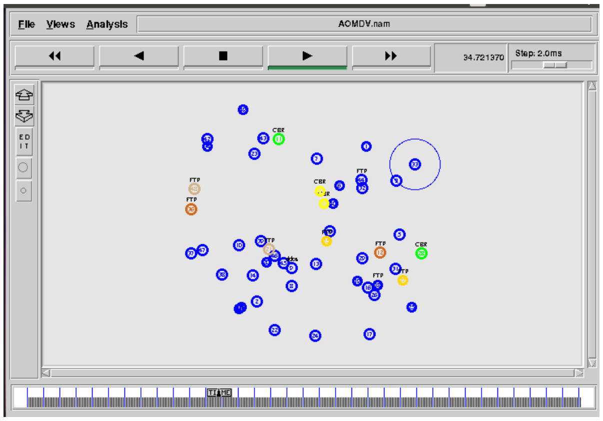

Figure 2: DDoS prevention in network.

Because of proposed algorithm the detection and prevention of the DDoS attack is achieved in the network. The above figure represented the detection and normal data transmission in the network.

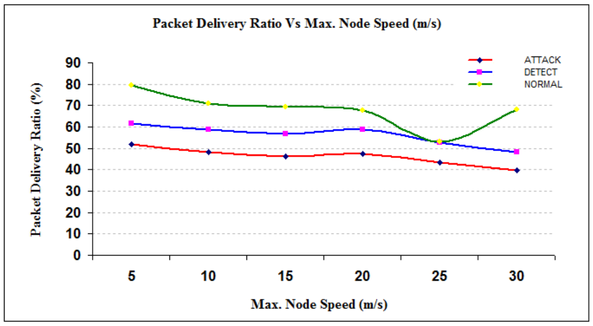

Figure 3: Packet Delivery Ratio (%) Vs Max Node Speed (m/s)

In the above graph where the data sending ratio is designed alongside the node motion we observe that AODV performs better in low node mobility rate while as the mobility amount rises the distribution ratio to some extent dew drop. The performance of the system is similarly expressively condensed when AODV is under the DDoS attack and the node mobility increases. However, this behavior is normal for the purpose that by way of the node movement upsurges the system network topo-logy variations making nodes lead RREQ packets more frequently, and therefore the malicious node has the opportunity to send more false RREP packets to the increased route requests that are sent to cope with the route changes.

V. CONCLUSIONS

MANET network using AODV under distributed denial of service malicious attack with secure routing and data transmission is proposed in this paper. The experimental outcome represented DDoS prevention and detection scheme with improved performance in the network. The proposed scheme is well appropriate for mobile network security. The proposed system is planning to implement in real environment and evaluate the network performance. A direction of future investigation is to use better encryption scheme to secure data transmission in distributed denial of service attack.

REFERENCES

[1] National Science Foundation Research priorities in wireless and Mobile communications and Networking: Report of workshop held March 24-26,1997,Airlie House,Virginia.Available at http://www.cise.nsf.gov/anir/ww/html

[2] Pravin Ghosekar, Dhanwante National college, Girish Kathkar, Dr.Pradip Ghorpode," Mobile Ad-hoc networking: impartaive and challenges,IJCA Special Issue,"Mobile Ad-hoc Network" MANETs 2010.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE 2002, pp-433-445

[4] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2114

[5] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.

[6] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, " On a mathematical model for low-rate shrew DDoS," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.

[7] G. Macia-Fernandez, J. E. Diaz-Verdejo, and P. Garcia-Teodoro, "Mathematical model for low-rate DoS attacks against application servers," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 519–529, Sep. 2009.

[8] Zhijun Wu, Liyuan Zhang, and Meng Yue , Low-Rate DoS Attacks Detection Based on Network Multifractal, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL.

[9] U. Venkanna, R. Leela Velusamy, Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks, IEEE 2015, pp 223-234

[10] Wenjia Li, Anupam Joshi, Tim Finin, CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies, IEEE 2010, pp-188-201

[11] A. Feldmann, A. Gilbert, and W. Willinger, "Data networks as cascades: Explaining the multifractal nature of internet traffic," in Proc. ACM SIGCOMM, Sep. 1998, pp. 42–55.

[12] Z. Xia, S. Lu, and J. H. Li, "DDoS flood attack detection based on fractal parameters," in Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput., 2012, pp. 1–5.