Security Improvisation Of Mac Layer In Mobile Ad Hoc Networks

Deepika Malviya, Dr. Prashant Sharma, Ankita Bhargava

Abstract: MANET became most popular and employed wireless networks. In MANET, hubs utilizes remote connects to interface each other in a system MANET is part of dynamic type of network as it deploy non-fixed infrastructure, dynamic topology, absence of central administration which can provide assistance to all nodes of network and self configured. Principle focal point of our examination is DoS recognition and presentation of different strategy for suspension of attack. A framework is structured which joined the upper side of various methodologies and attempted to deal with all aspects of DoS attack. Our system work in three layer i.e. Monitoring, Detecting and Suspending (MDS). In Monitoring stage identification of whether network is suffering from any attack or not is done. In detecting stages, types of different attacks are classified and many ways to deal with are devised. In third step i.e. Suspension methods are enrolled to either remove the nodes from network which misbehave or introduce new feature such that nodes cannot easily introduce DoS attack. Such counter steps are taken such that malicious node are also forced to act in a proper way.

Keywords: Manet adhoc, Mac layer, Rts/Cts mechanism, Dos attacks

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are new networking which is emerging in wireless technology. In MANET, mobile nodes connect on improvised or ad hoc basis. It is self-healing and self-forming, provide communication facilities between different nodes of the network in the absence of centralized infrastructure. Mobile hosts which are loaded with wireless communication device come together to form mobile ad-hoc network (MANET). As mobile device are equipped with Omni-directional antennae due to which they have broadcast nature so any transmission done by any mobile host are received by every host in its transmission range. The host who are out of transmission scope of sending host gets information only when the other host who received data transmit to the hosts who are in his transmission range which result in effective wireless network forming among mobile host in a particular area. Every node of MANET has capability of working as autonomous system i.e. each node can perform routing their own without any need of central administration or any statically established infrastructure..Radio frequencies 30MHz-5GHz is communicating range of MANET.

2. LITERATURE REVIEW

Muralishankar and Raj, 2014, studied various routing protocols in MANET. these routing protocols are divided into three groups in MANET, that are reactive,proactive and hybrid. Under proactive protocol , each node discover route in advance before actually communication is requested .The proactive protocol cut down delay in time but increased the cost overhead.

- *Deepika Malviya, M.tech scholar, Department of computer science engineering, Pacific University, Udaipur, Rajasthan.*
- *Dr. Prashant Sharma, Head of Department, Department of computer science engineering, Pacific University, Udaipur, Rajasthan.*
- *Ankita Bhargava, Assistant Professor, Department of computer science engineering, Pacific University, Udaipur, Rajasthan*.

Mohseni et al., 2010, studied full comparison between proactive and reactive protocol. According to him In comparison to reactive protocol like AODV, proactive protocol have more control overhead and it include DSDV. Reactive protocol is considered as on demand protocol. Nodes are in sleeping mode they are activated only if a communication request arrives for other node. i.e. In reactive protocol network overhead in only one node but in that case time requirement is increased. Kyasanur & Vaidya (2005) have proposed the MAC layer misconduct through the modification of the IEEE 802.11 MAC protocol, in order to detect and penalize the selfish misconduct. Here authors suggested a new way ofassigning back off value by receiver to the sender by utilizing the control packets i.e. ACK and RTS. The assigned backoff value is used by sender in next transmission.

3. METHODOLOGY

Problem Statement

Some Important problem to be taken under consideration are:

- Packet forwarding
- Packet dropping
- Proper network link establishment from source to destination
- Trust establishment among node
- Efficient utilization of resources.

Proposed Methodology : MDS (Monitoring, Detecting and Suspending) Any misbehaviour node may lead to degradation of network performance. Their main focus is on concealing network's operation rather than on power saving. The MDS methodology works in three phases. During first phase it just monitors the whole network for any misbehaving node. Now some new techniques are introduce for detecting different attacks and arrival of third phase which introduce some new fields and exchange of some message to Suspend attack.

(1) Monitoring

The Monitoring phase simply looks on network activity for searching a malicious node. The following activities in

network may point to malicious behavior node and network.

(2) Detection

The main role of this stage is pointing out malicious node .

- **TO attack:** This attack was already detected and discovered by Guang and Assi.(2006). This attack basically carried out by modifying three timeouts i.e. CTS, DATA and ACK. Sender after sending RTS wait for CTS signal. After sending RTS, node waits for calculated time for CTS signal and after receiver sends CTS signal it waits for pre-calculated time for DATA from sender. Sender after sending DATA waits for pre-calculated time for ACK signal. This attack can be either done by sender or receiver side node.

(3) Suspending

Suspension means creating barriers to overcome attack.

- To deal with TO attack when sender sends RTS than it will include one more field in its frame format i.e. TO field each time between sender and receiver when handshake mechanism and data transmission is done its other side will tell the former side about how much time it has to wait before former Time Out. One more thing when node receives a TO value it will match with its own calculated value when it is less than,it will set its own value else set the frame format value. Steps for Overcome TO attack is:
  - ✓ Sender will send RTS signal along with introducing a new field field in frame i.e. TO to value calculated by equation

    $TO = 4\delta + 2SIFS + T_{CTS} + H$

    WHERE,

    δ is propagation delay, SIFS is shortest time for which sender waits before sending data and after receiving CTS and receiver waits for after receiving RTS and DATA . T_{CTS} is time to travel CTS signal and H is time to travel data header.
  - ✓ Sender will wait for following time for CTS signal:

    $TO_{CTS} = T_{RTS} + 2\delta + SIFS + T_{CTS}$
  - ✓ Receiver will check TO field with its calculated TO time if it is greater than or equal to its calculated time than it will set the same value for itself to wait for next signal else it will declare node as malicious node who is trying to perform TO attack.

4. RESULT AND DISCUSSION

Exp

Number of nodes	*10,15,20,25,30*
CWmin	*3*
CWmax	*63*
DIFS	*34 µs*
SIFS	*16 µs*
Slot time	*9 µs*
Routing Protocol	*AODV*
Traffic Type	*TCP*
MAC Protocol	*IEEE 802.11*

Simulation of algorithm is done by using Network Simulator-2 (NS-2). In this we carried out experiment by taking different nodes i.e. 25, 35, and 45. Simulation area is 1200*1200. The data rate of of 2 Mbps sre used by propagation channel of two ray ground reflection model. Experiment is carried out in a fixed area if any node is outside the boundary it will consider as out of the network and communication establish with the node. Source transmits Constant Bit Rate (CBR) with UDP traffic at two frames per second and data payload of each frame is100 bytes long. Source. Mobile nodes are moved arbitrarily according to the desultory waypoint mobility model with the node speed of 2 m/sec. AODV routing protocol is utilized to find the path for a given source-destination pair (Perkins and Royer 1999). Table1 Simulation Parameters

Experimental results

We fixed presence time to 1 sec of malicious node is fixed to 1sec. The total number of nodes present in the network is 10,15,20,25,30 and number of malicious nodes in the network is 0, 1 and 3. The packet delivery ratio is decreased as the no. of malicious nodes is increased. When we introduce malicious node and increase the no. of node than with increase in no. of node packet delivery ratio increased. Firstly, generate trace file running the Tcl source code. After executing the command “gawk -f awkfilename tracefilename” in different scenarios, it is revealed that Packet delivery ratio is 100% when nodes are increased from 10,15,20,25,30. This is shown below in graph which run the awk script alongwith trace file

Scenario 1: comparision between MDS and IEEE 802. values

No. of nodes	*PDR of IEEE 802.11*	*PDR of MDS*
10	*100*	*100*
15	*100*	*100*
20	*100*	*100*
25	*100*	*100*
30	*100*	*100*

Table 2 : *PDR in 10,15,20,25,30 node network without malicious node*

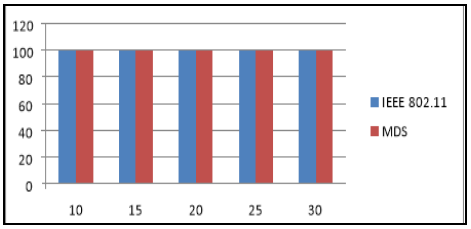

Fig 5 : *Chart of PDR in 10,15,20,25,30 node network without malicious node*

Scenario 2: *Comparision Of MDS and IEEE 802.11 PDR when 1 malicious node present*

No. of nodes	*MDS*	*IEEE 802.11*
10	*86.655*	*84.336*
15	*86.767*	*84.563*
20	*86.908*	*84.765*

25	*87*	*84.965*
30	*87.333*	*85.121*

Table 3: *Comparison Of MDS and IEEE 802.11 PDR when* 1 malicious node present

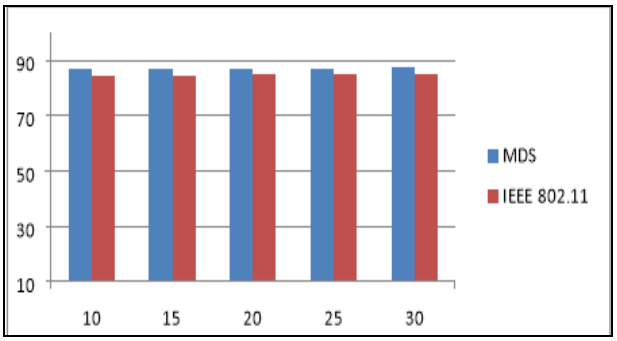

Fig 6 : *Chart for Comparison of MDS and IEEE 802.11 PDR when 1 malicious node present*

Scenario 3: Comparision Of MDS and IEEE 802.11 PDR when 3 malicious node present

No. of nodes	*MDS*	*IEEE 802.11*
10	*43.682*	*41.761*
15	*47.714*	*45.436*
20	*50.675*	*48.632*
25	*52.986*	*50.895*
30	*56.132*	*53.224*

Now, malicious node is introduce in Tcl source code and awk script is run to retrieve PDR and degradation in PDR occurs. Now, we introduce malicious node for 1 second in the network of different count of nodes 25, 35 and 45 nodes. Total time of experiment is carried out is for 10 seconds and malicious nodes are created between 3sec to 4sec period. The PDR in following situations is shown below .

Table 4: Comparison Of MDS and IEEE 802.11 PDR when 3 malicious node present

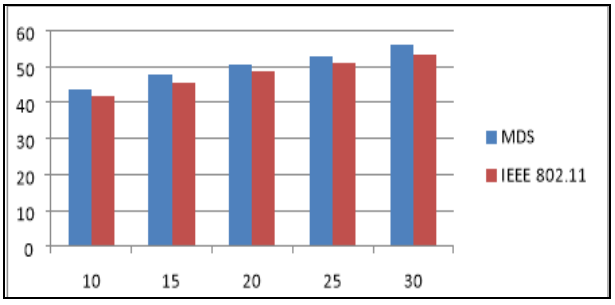

Fig 7 : Chart for Comparison of MDS and IEEE 802.11 PDR when 3 malicious node present

Now in Tcl source code no. of malicious node is increased from 1 to 3, and decrement in the PDR occurs. Here 3 malicious nodes are introduce in the network with 10,15,20,25, 30 nodes. The malicious nodes time is fixed in all node network in this experiment. After introduction of malicious node it is observed that with increase in no. of node PDR is n increased. Which can be viewed in above 3 chart, it is observed that when number of nodes are increased after introduction of malicious node in network the PDR is also increased. It is clear from above figures with increase in no. of malicious node PDR decreases

5. CONCLUSION AND FUTURE WORK

The MDS i.e. Monitoring, Detecting and Suspending used to deal with various attack. Firstly,it check for malicious sender who waste network bandwidth or we can say slow down whole network through sending continuous Hello messages. It also check for malicious activity of node who overwhelm receiver. Lastly in suspending stage steps are taken to deal with TO attack using new field in frame format. There is immense emergence to use mobile ad hoc network in various field. Manet can be used in different field like healthcare, education, defense etc. The attack power is increased if malicious node increased providing favorable condition to decrease network security. In our research we proposed method to first monitor the attacks from malicious node then detect node as malicious one and then we suggested a new way for suspension attack. Sothat malicious node is forced to behave properly. As all protocol are implemented in the form of software rather hardware so it become easier to modify the predefined rules. MDS pointed out different security measures and also suggested the prevention methodology as countermeasure of DDOS vulnerable MANETS.

6 REFERENCES:

[1] Chaminda Alocious, Hannan Xiao and Bruce Christianson 2015. Analysis of DoS Attacks at MAC Layer in Mobile Adhoc Networks.The International Wireless Communications & Mobile Computing Conference IWCMC 2015), At Dubrovnik, Croatia, Volume: 11978-1- 4799-5344-8/15 2015 IEEE

[2] Yao J. at el, Revisiting of Channel Access Mechanisms in Mobile Wireless Networks through Exploiting Physical Layer Technologies; Wireless Communications and Mobile Computing; Vol(2018); PP16; (2018).

[3] Kyasanur P and Vaidya NH, Selfish MAC layer misbehavior in wireless networks, IEEE Transactions on Mobile Computing, vol. 4, no. 5, pp. 502-516 (2005).

[4] Mishra A and Nadkarni KM, Security in wireless ad -hoc network, CRC press LLC (2003).

[5] Murthy SR and Manoj BS, Ad hoc wireless networks, architectures and protocols, Second Ed., Low price Ed., Pearson Education (2007).

[6] Perkins CE and Royer EM, Ad hoc on-demand distance vector routing, Proceedings of the 2nd IEEE workshop on mobile computing systems and applications, New Orleans,pp. 90-100 (1999).

[7] Srivastava P and Singh D, A Survey on Modified RTS/CTS Mechanism, International journal of computer network and wireless communication, vol. (3), pp. (13-18), (2013).

[8] Radosavac S; Moustakides GV; Baras, JS and Koutsopoulos, I, An analytic framework for modelling and detecting access layer misbehaviour in wireless networks, ACM Transactions on Information and System Security (TISSEC), vol. (11), no. 4, pp. 1-27 (2008).

[9] Rai D; Sharma S and Naznee S, Optimized RTS/CTS exchange approach for better performance in multi hop WLAN environment, International journal of advanced research in computer and communication engineering, vol.(1), issue (6), pp. (454-459), (2012).

[10] Rajput P; Chauhan J and Dhaybhai K, Detection technique for the timeout MAC layer misbehavior in mobile adhoc network, International journal of research culture society,vol. (2) PP. 476-483 (2018)

[11] Guang L and Assi C, A self-adaptive detection system for MAC misbehaviour in Ad Hoc Networks, Proceedings of the IEEE international conference on communications, ICC,vol. 8, pp. 3682- 3687 (2006,).