IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 4, Ver. I (Jul-Aug. 2014), PP 32-38
www.iosrjournals.org

Enhanced Adaptive Acknowledgement Method for Detecting Malicious Nodes in MANETs

Akshatha.Y[1], Dr Rashmi M.Jogdand[2]
[1](*M.Tech 4th semester, Department of CSE, KLS Gogte Institute of Technology, Belgaum, India)*
[2](*Professor, Department of CSE, KLS Gogte Institute of Technology, Belgaum, India)*

Abstract : *Mobile Ad hoc Network is a collection of mobile nodes that communicate with each other without base station. These networks are developed instantly or on-demand when some nodes come in the mobility range of each other and decide to cooperate for data transfer and communication. MANETs are more vulnerable to various types of attacks due to its deployment nature. The security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics such as dynamic topology, open medium, limited power, limited bandwidth and remote transmission. The prevention mechanisms like cryptography or authentication alone cannot detect malicious nodes in Ad-hoc networks. Hence we propose and implement a new intrusion detection system named Enhanced Adaptive Acknowledgement method specially designed for MANETs. Using MRA scheme, this method is capable of detecting malicious nodes even in the presence of false misbehavior report. Compared to other detection methods, this method is capable of detecting high malicious nodes and hence increases the security and network performances.*

Keywords: *Mobile ad-hoc network, Intrusion detection system, Enhanced Adaptive Acknowledgement, AODV, MD5 hash algorithm.*

I. Introduction

Mobile ad hoc network (MANET) is a new emerging technology which enables users to communicate without using any fixed or physical infrastructure. In Mobile ad hoc network, different wireless mobile devices are working as a mobile node that build virtual network infrastructure without any centralized server for wireless communication. Each device in a MANET is free to move separately in any direction in any space, and will therefore change its links to other devices regularly. Mobile nodes are equipped with a wireless transmitter and a receiver that communicate directly with each other or forward message through other nodes. MANETs are highly vulnerable to attacks than wired networks due to the open medium and changing topology.

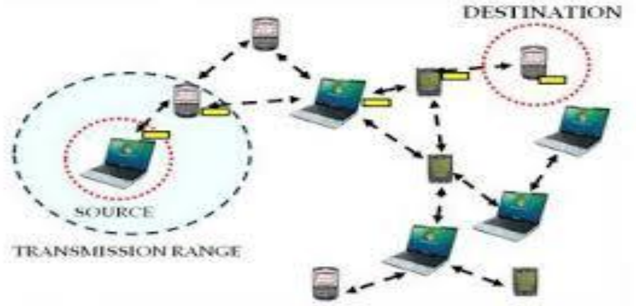


Fig 1: Mobile Adhoc Network

Security in an infrastructure-less ad hoc network is a great challenge[2]. At the same time the resources such as limited power, limited communication range, processing capabilities, and limited memory of the Mobile Ad hoc network maximize the total network throughput by using all available nodes for routing and forwarding. Hence, a node can misbehave and fail to establish route due to its malicious activity to decrease the performance of mobile ad hoc network.

1.1 Intrusion Detection System

Different types of intrusion detection Systems are developed for detecting the malicious nodes in the wired networks. Due to the mobility of nodes and changing topology, the intrusion detection techniques of wired network cannot be used for MANETs. An intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized entry and/or malicious activity. The way that an IDS detects anomalies can vary widely; however, the ultimate aim of any IDS is to catch attackers in the act before they do real damage to resources [3]. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. Depending on the detection methods it chooses to deploy, there are several direct and incidental benefits to using IDS. An Intrusion detection uses vulnerability assessment, which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- ✓ Monitoring and analyzing both user and system activities.
- ✓ Analysis of abnormal activity patterns.
- ✓ Analyzing system configurations and vulnerabilities.
- ✓ Ability to recognize patterns typical of attacks.
- ✓ Assessing system and file integrity.
- ✓ Tracking user policy violations.

Understanding what an IDS is and the functions it provides, is key in determining what type is appropriate to include in a computer security policy. It explains the concepts behind IDS, the functionalities of each type of IDS, and the emergence of hybrid IDS that employ several detection techniques and tools in one package.

II. Literature Review

Marti et al. [4] proposed a scheme named Watchdog that helps to detect misbehaving nodes and enhance the throughput of network with the presence of malicious nodes. In reality, the Watchdog scheme consisted of two different parts, namely, Watchdog and Path rater. Watchdog serves as an ID for MANETs and it is responsible for detecting the malicious node misbehaviors in the network. Watchdog detects the malicious misbehaviors by listening to its next hop’s transmission. If Watchdog node overhears that its next node fails to forward the packet within a definite period of time, it increases its failure counter. Whenever a node’s failure counter exceeds a predefined threshold value, the Watchdog node informs it as misbehaving node. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many research studies and implementations have proved that the Watchdog scheme is effective. Besides, compared to some other schemes, Watchdog is competent of detecting malicious nodes rather than links in the network. These advantages have made the Watchdog scheme a popular choice in the field. Nevertheless, as pointed out by Marti et al. [4], the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following ie. Ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report [5].

With respect to the drawbacks of the Watchdog scheme, many researchers proposed various approaches to solve these issues. TWOACK proposed by Liu et al. [5] is one of the most significant approaches among them. On the contrary to many other schemes in detecting malicious nodes, TWOACK is neither an enhancement nor a Watchdog-based scheme to detect malicious nodes. Aiming to resolve the receiver collision and limited transmission power of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node down the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. The same process applies to every three consecutive nodes down the rest of the route [10]. The TWOACK scheme successfully solves the receiver collision and limited transmission power faced by Watchdog [9]. Though, the acknowledgment process required in every packet transmission process added a major amount of unwanted network routing overhead. Owing to the limited battery power nature of MANETs, such unneeded transmission process can easily degrade the life span of the entire network. The main disadvantage of TWOACK technique is Routing overhead.

Based on TWOACK, Sheltami et al. [6] proposed a new scheme that is called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be used as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK considerably reduces network overhead while still capable of maintaining the same network throughput during data transmission [10]. Within a predefined time, if the source node S receives this ACK acknowledgment packet from the destination node, then the packet transmission from node S to node D is successful. Or else, the source node S will switch to TACK scheme by sending out a TACK packet.

III. Secure Ids Description

It is highly vital to guarantee that the data packets are valid and authenticated in the existing system. In order to ensure the integrity of the IDS, IDS requires data packets to be encrypted before they are sent out and verified until they are accepted. To address the problem of extra resources required due to the introduction of security in MANETs we adopt a security in our proposed method namely Enhanced Adaptive Acknowledgement to achieve the goal of finding the most optimal solution for using security in MANETs. It is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In this secure ID, It is assumed that the link between each node in the network is bidirectional[8]. Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

1) ACK: ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS aiming to reduce network overhead when no network misbehavior is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

2) S-ACK: It is an advanced version of the TWOACK IDS [6]. The objective is to let every three consecutive nodes work in a group to detect malicious or misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The main goal of introducing S-ACK mode is to detect malicious nodes in the presence of receiver collision or limited transmission power.

3) MRA: Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior.

The MRA field is designed to solve the weakness of Watchdog when it fails to detect malicious nodes with the presence of false misbehavior. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The mail goal of MRA field is to authenticate whether the destination node has received the reported missing packet through a different route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes [9]. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

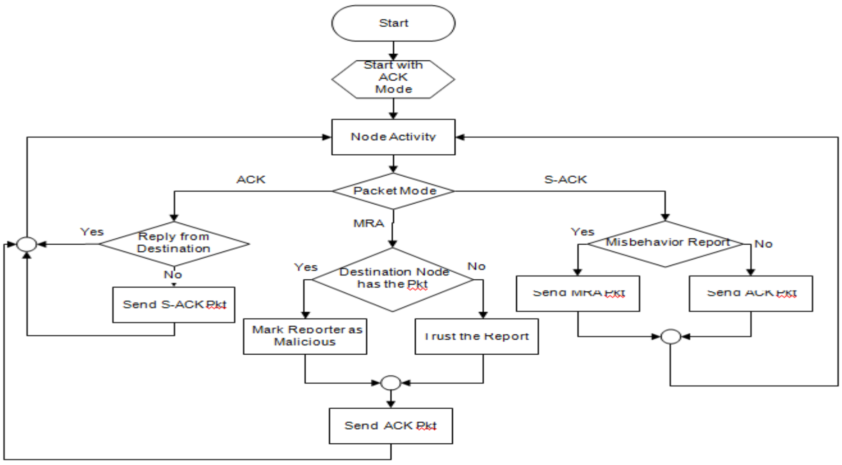


Fig 2: System Architecture

This method uses AODV routing protocol to find the shortest path in the network to reach the desired destination. Then it encrypts the data packet with hash key and send to the destination. The destination decrypts the data and check the hash value for data integrity. If the route has attacker nodes and if the sender does not receive acknowledgement packets then the packets will be sent in the new route. If any node wants to send packet to neighboring node then first source node generate the packet and send to the neighboring node[9]. The packet is sent to acknowledge system in which we use AACK with security. After that it send packet according to mode and detect the attacker in the system, If malicious or misbehaving node is detected then alert will be triggered by the same node that detect the misbehaving node. When a node detect malicious node it will inform the source node by sending an acknowledgement, which is a small packet that is generated by the routing protocol and extract the route from source route of corresponding data packet and the packet will be sent in a new route.

IV. Performance Evaluation

4.1 Simulation model

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on fedora. The system is running on a laptop with 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 500 × 500 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 200 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, we ran every network scenario three times and calculated the average performance.

Table 1: Simulation Parameters

Sl.No	**Parameter**	**Value**
1	Number of nodes	50
2	Simulation Time	10sec
3	Packet size	512bytes
4	Routing Protocol	AODV

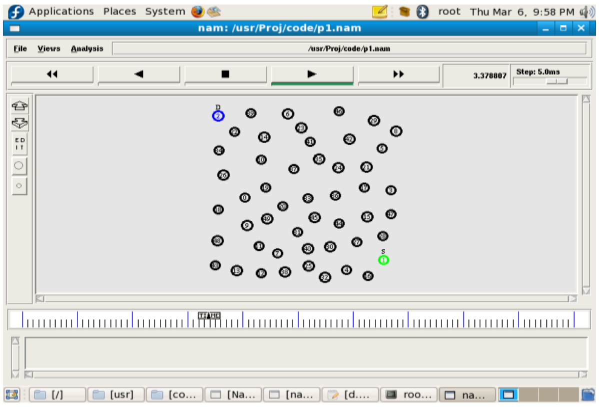
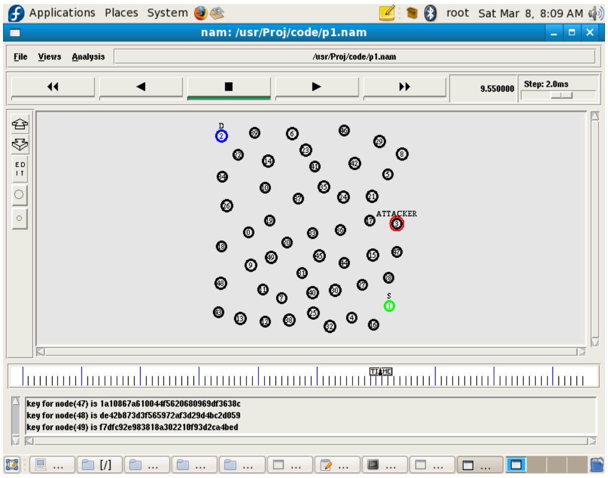


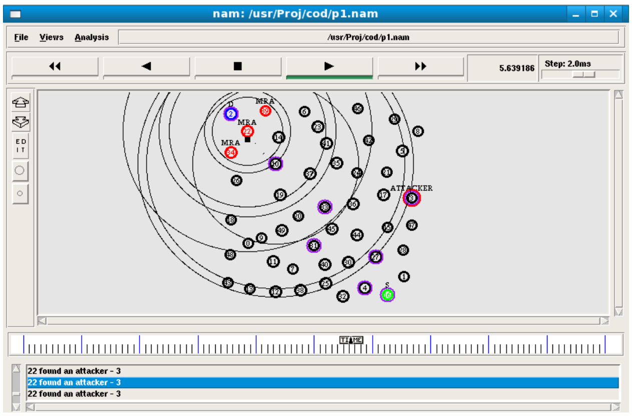
Fig 3: Snapshot of node deployment

Fig 3 shows that simulation of node deployment. Here 50 nodes are deployed. As shown in above snapshot node 1 and node 2 marked with red and blue circle are indicated as source and destination nodes respectively.



```
key for node(47) is 1a10867a610044f5620680969df3638c
key for node(48) is de42b873d3f565972af3d29d4bc2d059
key for node(49) is f7dfc92e983818a302210f93d2ca4bed
```

Fig 4: Snapshot of Key generation



```
22 found an attacker - 3
22 found an attacker - 3
22 found an attacker - 3
```

Fig 5: Snapshot of MRA which detects false misbehavior report and drops malicious nodes

4.2 Performance metrics

These following metrics are used to evaluate the performance for existing and proposed technique which is defined as follows:

4.2.1 *Throughput:*

Throughput is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network The average rate of successful message is delivery over a communication channel.

4.2.2 Average end to end delay:

The average end-to-end delay is calculated for all successfully received packets at the destination. It is calculated for each data packet b subtracting the sending time of the packet from the received time at final destination. Then the average represents the AED.

$$AED = \frac{\sum_{1}^{N}(T_{Rceived} - T_{Sent})}{N}$$

4.2.3 Packet delivery ratio (PDR)

It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

Scenario 1: Throughput

Table 2: Pause time Vs Throughput

PAUSE TIME	Throughput varying no of flows AODV	 DSR
0	551.254	600.356
5	623.49	786.247
10	753.65	864.12
15	803.95	945.36
20	921.354	1001.621
25	684.84	921.154
30	620.87	847.164

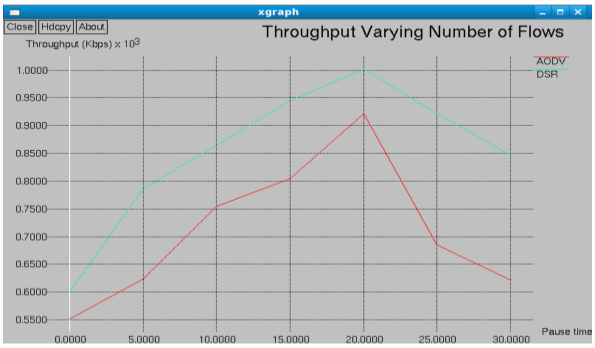


Fig 6: Throughput varying number of flows

As the load increases both on-demand protocols works better compared to DSR. Throughput of AODV is high at higher traffic load where as DSR performs well at moderate traffic. The reason is AODV adapts hop by hop routing whereas DSR adapts source routing.

Scenario 2: Average end to end delay

Table 3 Pause time Vs Avg End to End Delay

PAUSE TIME	Avg End to End delay	
	AODV	DSR
0	27.5	15
25	11	14.8
50	12	13
75	10	14.5
100	14	14.6
125	14	15
150	11	12.6

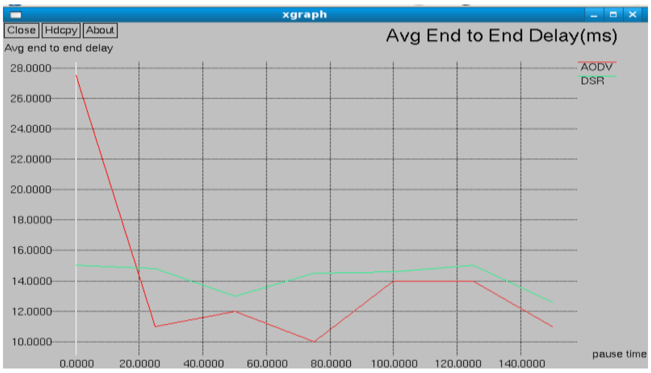


Fig 7: Avg End to End delay

As traffic load increases AODV performs better as it adopts hop-by-hop routing. DSR performs better at lower and moderate traffic load as it uses source routing.

Scenario 3: Packet delivery ratio

Table 4: Pause time Vs Packet delivery ratio

PAUSE TIME	Packet delivery ratio *10^3(%)	
	AODV	DSR
0	0.82	0.9
1	0.8	0.98
2	0.75	0.98
3	0.77	1.0
4	0.84	0.98
5	0.874	1.0
6	0.901	0.99
7	0.96	0.91
8	1.0	0.99
9	1.01	0.9

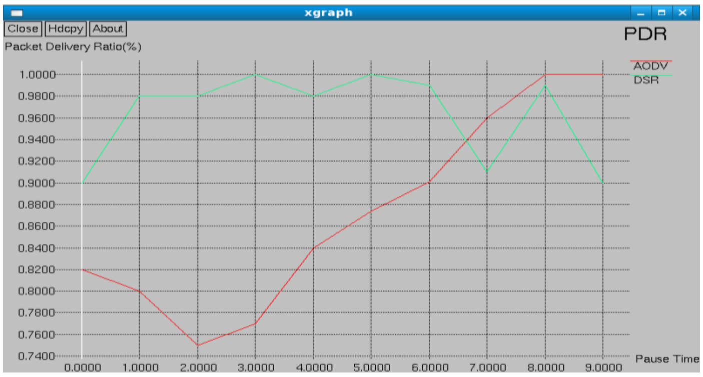


Fig 8: Packet delivery ratio (PDR)

AODV and DSR build the routing information as and when they are required to send data. This makes them more adaptive and results in better performance with respective to high packet delivery fraction .AODV delivers more packets at high traffic load compared to DSR.

V. Conclusion

Enhanced adaptive acknowledgement method makes MANETs more secure. Major problems such as forged acknowledgement and malicious modes can be detected using this method. It also solves weakness such as receiver collision and limited transmission power and also proves transmission is authentic. This method is designed especially for MANETs and compared it against with previous approach in different scenarios through simulation. We got positive results when proposed AODV protocol is compared with previously used DSR protocol in different scenarios such as Packet delivery ratio, Throughput, Average end to end delay and routing overhead. Authentication based Digital Signature scheme is incorporated in order to prove the secure transmission of packets in network and to detect malicious nodes at maximum extent.

Acknowledgements

I give my sincere feelings of thankfulness to Dr.Rashmi M.Jogdand for her valuable guidance ,support and encouragement which helped me a lot to write this paper and also other faculty members of KLS Gogte institute of Technology, Belgaum for their valuable suggestions and comments that helped to improve the quality of article.

References

[1] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE

[2] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[3] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999.

[4] [5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[5] "A study of different types of attacks on multicast in mobile ad hoc networks" Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier AdHoc Networks(2008) 32-46. [7] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[7] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[8] A. Tabesh and L. G. Frechette, "A low-power stand- alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[9] A. Tabesh and L. G. Frechette, "A low-power stand- alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[10] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks:Challenges and solutions" (2004). IEEE Wireless Communications.