A Novel Approach towards the Detection of Malicious Nodes in Mobile Ad Hoc Networks

Anup Ashok Patil
Department of Electronics & Telecommunication
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai
University of Mumbai

Shital Mali
Department of Electronics & Telecommunication
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai
University of Mumbai

ABSTRACT

Mobile Ad hoc Network (MANET) is a group of wireless nodes that cooperatively form a network without any pre – established or centralized infrastructural support.All the nodes in the network are moving independently within the same radio rangeand actsas hosts as well as routers. This network is vulnerable to number of attacks while doing data transmission throughout the network.MANETs are more vulnerable to attacks than traditional wired networks because mobile ad hoc network operates on different principles than that of the traditional networks. Security upto some extent is achieved by existing security mechanisms. To achieve acceptable level of the security, the existing security mechanisms should be combined with intrusion detection systems (IDS). There are some existing intrusion detection systems based on acknowledgement, but under certain circumstances these existing systems will not be able to detect the presence of malicious nodes effectively. So, a novel intrusion detection system called Secure Enhanced Adaptive Acknowledgement (SEAACK) is proposed in this paper. The proposed system deals with the issues related to the existing IDS and detect the malicious nodes more effectively than the existing system under certain circumstances while not greatly affecting the network performances.

Keywords

MANET, Secure Acknowledgement, Cryptography, False misbehavior, Intrusion Detection

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are formed from a collection of number of nodes, which are adjacent to each other in a certain range connected with wireless links. These networks have been proposed for the variety of applications such as collection of data in sensor arrays, disaster areas, hostile environment etc. There are mainly two challenges while creating such a network. Firstly, the network must operate independent of an access point infrastructure even though the connectivity between the nodes changes dynamically and unpredictably. Second, the network must operate independent of fixed or pre-established network management infrastructure while still providing administrative services needed to support applications [1].

As the network topology of MANET will not be fixed, the algorithms used for fixed topology will not directly used for the networks without a fixed topology and it should be changed according to the type of network. Due to the dynamic nature of MANET, they are widely used in military applications. These networks suffer from different security threats such as packet dropping, selfishness, black hole etc. [1].To deal with different security threats in the network, there must be some sort of security mechanism in the network. To deal with the issues related with some types of attacks, cryptographic mechanism are used for external entities but it cannot prevent the attack which is due to the internal entities present in the network which have rights to access the information of the network. So, to detect the internal malicious entities in the network an intrusion detection mechanism is necessary. Authentication and encryption are usually served as the first line of defense. However, a new security problem arises as the complexity of the system increases. To solve this problem we can use intrusion detection system as a second line of defense.

2. BACKGROUND

2.1 Vulnerabilities of MANET

The different vulnerabilities of MANET are as follows [1].

- Wireless Links.
- Dynamic Topology.
- Cooperativeness.
- Absence of a Clear Line of Defense.
- Limited Resources.

2.2 Types of Attacks

The classification of network Layer attacks in mobile ad-hoc networks is divided into two main divisions, known as passive attacks and active attacks [2]. Figure1 shows the classification of attacks in MANET.

2.2.1 Passive Attacks

It attempts to learn or make use of the information from the system but does not affect the system resources. From Figure1 we can conclude that passive attack consists of location disclosure, traffic analysis, eavesdropping. In traffic analysis, an attacker gains the knowledge of data by observing the characteristics of communications that carry data. Also even if message contents are encrypted, an attacker can still determine identity and location of communication parties, observe the frequency and length of messages being exchanged and can guess the nature of communication [2]. Passive attacks are difficult to detect and should be prevented.

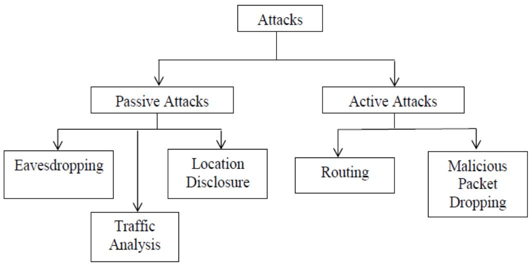

Figure1. Attacks in MANET

2.2.2 Active Attacks

It tries to change the resources of the system or affects their normal operation. Examples of active attack are Modification, Fabrication, Impersonation, Wormhole Attack,Black hole Attack, Lack of cooperation, Denial of Service (DoS) [2]. Active attacks are difficult to prevent and should be detected.

2.3 Related Work

Marti *et al.* [3] proposed a method named 'Watchdog' for the purpose of increasing the network throughput in presence of the malicious nodes.It consists of two parts merged for the detection of intrusion and response to intrusion if detected called Watchdog and Path rater respectively. Watchdog continuously monitors the network traffic and makes decisions based on listening to its next hop's transmission. If it came to know that its neighbor node fails to forward the packets within a predefined amount of time, it increases its failure counter and if this counter goes beyond some particular threshold, that node is declared as a malicious and misbehaving. Path rater is used along with the routing protocols to avoid the future transmissions to malicious or misbehaving nodes. The Watchdog scheme fails to detect malicious misbehaviors with the presence of ambiguous collisions, receiver collisions, and limited transmission power. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme, [4], [5], [6].

To deal with issues related to watchdog, TWOACK proposed by K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan [5]. It is used to resolve problems related to the watchdog system.Sheltami *et al.* [6] proposed a new scheme called AACK. This system is based on the acknowledgements packets for the detection of malicious activities in the network. It consists of mainly two parts, time acknowledgement and another one is end to end acknowledgement. Since this system is based on acknowledgement packets for the detection of intruders, it is crucial to guarantee that the acknowledgement packets are valid and authentic.

3. IDS IN MANET

The mechanisms by which the monitoring of system activities will be done, these mechanisms are called as intrusion detection systems (IDS). First of all, all the activity information will be collected by IDS and by comparing those activities with the predefined normal activities, IDS will check the violation of security parameters. If it found some of the nodeswhich will not working according to their normal behavior and violating the security parameters, it alerts the system administrator and also it will take proper action in response to that abnormal activity [7]. Depending on the principle of operation and working, IDS are classified into two types, first one is host based and another one is network based. Host base IDS depends on the information available on host node while network based IDS depends on the network traffic information.

3.1 Stand-alone Intrusion Detection Systems

The name itself suggests that these types of IDS will run on each node individually for detection of intruders. These IDS works on individual nodes for the detection of malicious activities, so that there is no sharing of information among nodes about the type of malicious activities going on neighboring nodes [7]. The nodes in these IDS are not cooperative instead they are stand alone.These types of IDS rarely used due to its limitations that nodes are not cooperative and should not exchange the data among the network.

3.2 Mobile Agent for Intrusion Detection Systems

The main advantage of using mobile agents is that these mobile agents are able to move anywhere throughout a large network. More number of mobile agents are seamlessly distributed into the network performing several different tasks.The advantages of using the mobile agents in the network are discussed in [7]. It is not necessary to assign all functions to mobile agents instead some functions will not be assigned as per the requirements whichwill help to reduce the power consumption of the network.

3.3 Distributed and Cooperative Intrusion Detection Systems

As the topology of MANET is dynamic and distributed, so that it requires the cooperation from other nodes for the detection of intruders. The detection of intruders and in response to the detection of intruders, the system should be able to work in distributed manner and also it must be cooperative. Each node has an IDS running on it, whatever the data regarding the intrusion it will get, the nodes have to share this information to neighboring nodes and cooperatively participate in the detection of intruders in the network [8]. These types of IDS can be used in multilayer architecture.

3.4 Hierarchical Intrusion Detection Systems

The distributed networks uses these types of IDS in which the network regions are distributed in different clusters and consisting of multilayers [8].Cluster heads have to play a very crucial role in these types of networks since cluster heads responsible for monitoring the network activities and response when any of the intruders is detected locally and globally.

4. METHODOLOGY

This section describesSEAACK scheme in detail. Figure2 presents a flowchart describing the SEAACK scheme. The description of incorporated methods in proposed mechanism is described by following subsections

4.1 Acknowledgement (ACK)

This is an end to end acknowledgement method[6]. It is a part of a proposed system which is used to reduce the network overhead when there is no misbehavior spotted in the network. In this mode, first the source node sends an acknowledgement data packet to the destination through intermediate nodes by adopting the smallest route to the destination. After receiving the packet, the destination node sends the reply acknowledgement packet to the source within a predefined amount of time, so that source node confirms that the data packet received at the destination.

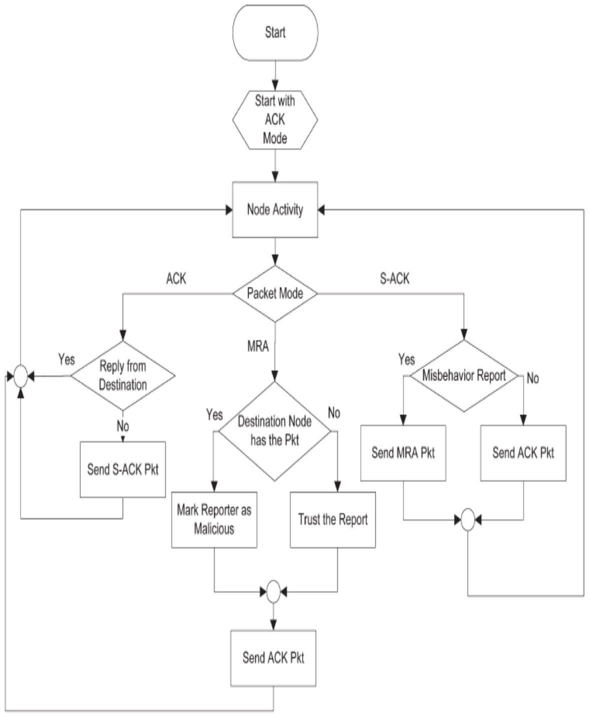

Figure2. Proposed Algorithm

4.2 Secure Acknowledgement(S-Ack)

It is the extended version of TWOACK scheme proposed by K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan [5]. In this system every three adjacent nodes works together for the detection of malicious activities. For every three adjacent nodes in the route, first node sends data packet to third node and upon receiving the data packet the third node will have to send S-ACK packet to first node. Let X, Y, Z are three adjacent nodes inthe network. Node ‘X’ sends S-ACK data packet to node ‘Y’ and node ‘Y’ send this to node ‘Z’. After receiving the data packet node ‘Z’ is required to send back S-ACK acknowledgement packet to node ‘Y’ and finally to node ‘X’ in a predefined amount of time. If the acknowledgement is not received in a predefined amount of time node ‘X’ treats that node ‘Y’ and node ‘Z’ are malicious and also give misbehavior report to the source. It is very difficult whether to trust the misbehavior report or do not trust the report, because it may also be came from one of malicious node. So, to deal with this issue, misbehavior report authentication scheme will be used which is explained in next section.

4.3 Misbehavior Report Authentication (MRA)

The false misbehavior report can be generated by nodes which are not behaving according to their normal behavior, to falsely report normal behaving nodes as abnormal and malicious nodes. The main cause to deploy MRA is for the authentication of received misbehaving report[9]. In this scheme, first source nodes finds an alternative path to the destination based on local knowledge and if it does not find any route then starts requesting another route based on protocols. Due to the dynamic nature of MANET, it is easy to find more than one route from source to destination. By adopting this new route we can be able to detect the node which generates the false reports. When MRA packet reaches at the destination, it searches if the reported packet was received and compares in order to take final decision. If it is received then the decision is made on the basis of this, that the node is not misbehaving otherwise it is misbehaving.

4.4 Digital Signature Algorithm

As proposed system is based on acknowledgement packets and all three parts of systemexplained in above sectionsare acknowledgment-based detection schemes. For the detection of malicious misbehaviors they are dependent on the acknowledgement packets. It is crucial to guarantee that the acknowledgment packets are valid and authentic otherwise all the schemes are vulnerable to forge acknowledgement packets by the attackers. So to maintain the integrity of the intrusion detection system, before sending the acknowledgement packets have to be digitally signed and verified until they are accepted. To achieve this goal digital signature algorithm (DSA) is implemented in our proposed system [10].

5. PERFORMANCE EVALUATION

In this section, the simulation platform,different simulation parameters, and performance metrics which will be used for analysis of proposed system are explained.

5.1 Simulation Setup

For simulation, network simulator (NS2) version 2.33 running on Rad Hat Linux [11] is used.

5.2 Performance Metrics

5.2.1 Packet Delivery Ratio

$$\boldsymbol{PDR} = \frac{\sum \boldsymbol{Packets\ received\ at\ the\ destination}}{\sum \boldsymbol{Packets\ sent\ by\ \ the\ source}}$$

5.2.2 Routing Overhead

$$RoH = \frac{\sum Routing\ Trassmisssion}{\sum Data\ Transmission + \sum Routing\ Transmission}$$

Table 1: Simulation Parameters

Channel	Channel/ Wireless Channel
Propagation	Propagation/ Two Ray Ground
Network Interface	Phy/ Wireless Phy
Medium Access Control (MAC)	MAC/ 802_11
Interface Queue Type	Queue/Drop tail/Pri queue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Interface Queue Length	50
Number of mobilenodes	32
Simulation Area Size	1000*550
Time of simulation	50 sec
Traffic Pattern	CBR
Platform	Rad Hat Linux 6

5.2.3 Throughput

It is the amount of data received at the destination.

5.3 Simulation Results

This section describes the comparison between the existing systems with proposed system based on different performance matrices stated in above section.

5.3.1 Packet Delivery Ratio

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. From Figure3, proposed system ensures maximum packet delivery ratio which is highlight with yellow color.

5.3.2 Routing Overhead

Routing Overhead defines the ratio of the amount of routing related transmissions. There is slight increase in routing overhead of proposed system due to adaptation of alternate path during the detection of misbehavior report as well as due to digital signature which is highlighted with yellow color in Figure4.

5.3.3 Throughput

The amount of data received at the destination is more than that of existing system which is highlighted with yellow color as shown in Figure5.

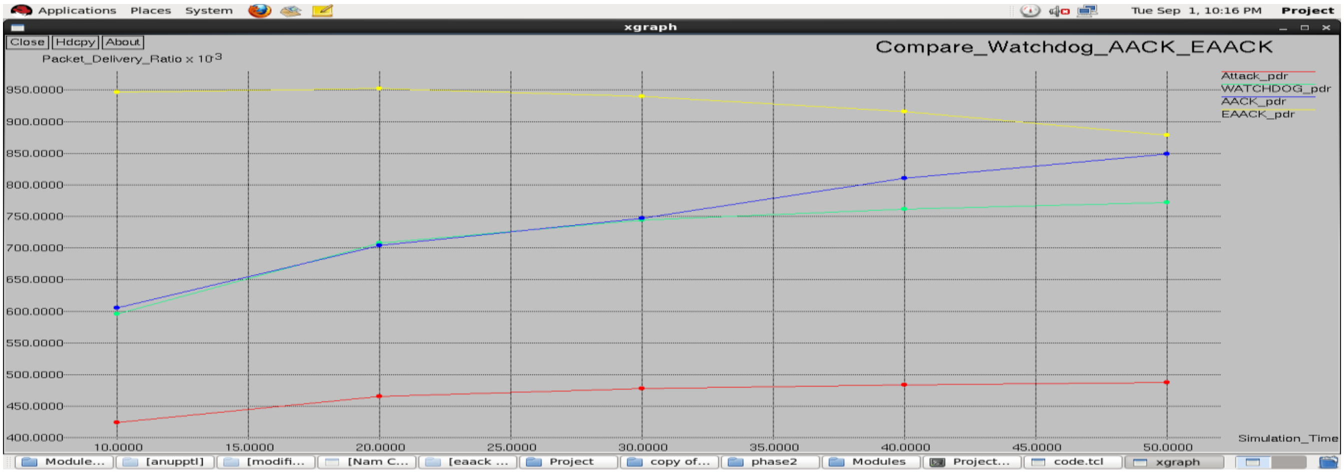

Figure3. Packet Delivery Ratio

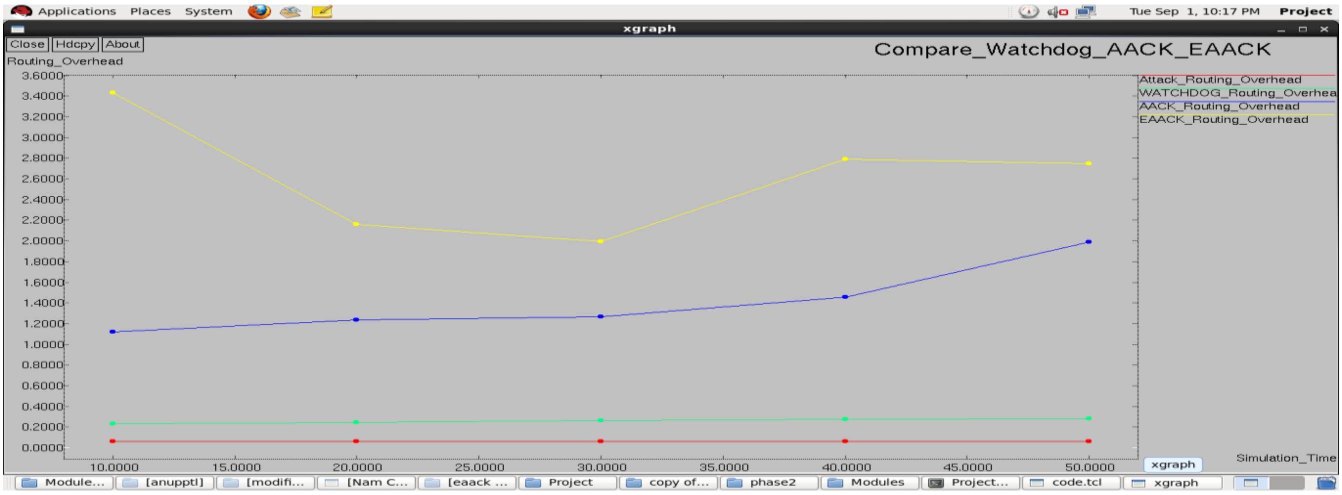

Figure4. Routing Overhead

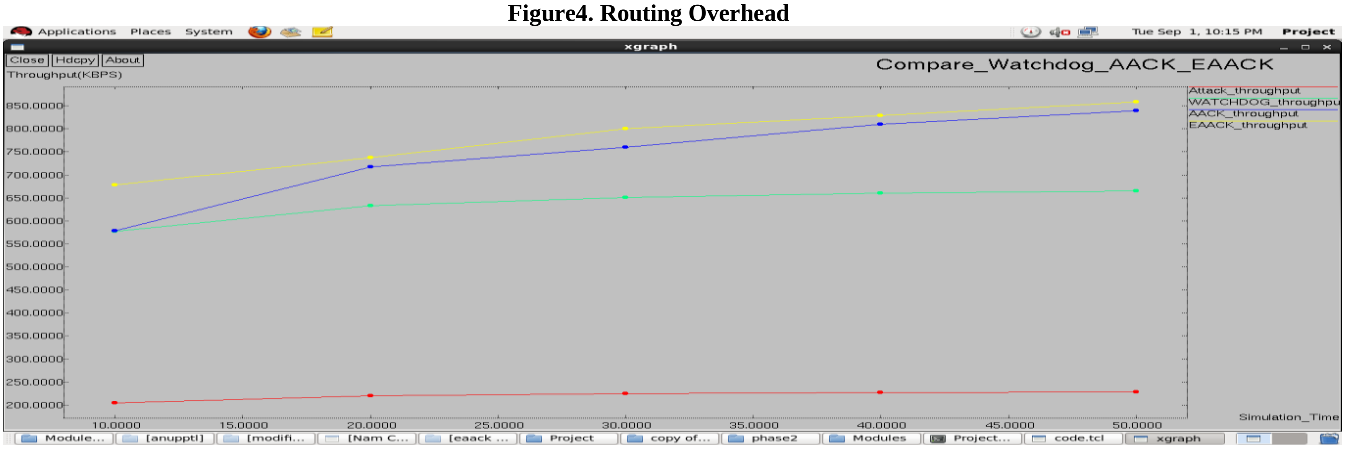

Figure5. Throughput

Table 2: Simulation Results

Simulation parameters	Watchdog	AACK	SEAACK
Packet Delivery Ratio	0.63	0.71	0.94
Routing Overhead	0.21	1.73	2.62
Throughput (kbps)	546.97	623.93	780.8

6. CONCLUSION AND FUTURE SCOPE

In this paper, the secure protocol is designed for detection and prevention of the presence of malicious activities in mobile ad hoc networks to enhance the network performances. From obtained simulation results following conclusion can be drawn. Firstly, proposed system exhibits higher packet delivery ratio of about 94%which is far better as compared to other existing systems. Second, the throughput which is nothing but the amount of data received at the destination of proposed system is much greater of about 780.8 Kbps than the existing systems. Third, routing overhead which is ratio of amount of routing related transmissions, supposed to be as small as possible for better network performance but there is slightly increase in the routing overhead of proposed system which is 2.62 due to the adaptation of digital signature.Though by adaptation of digital signature there is increase in network overhead, it is acceptable as compared to other systems as it will increase the packet delivery ratio of the network, when the attackers are smart enough to forge acknowledgment packets.Therefore from the analysis of above results it is cleared that proposed system is more suitable and efficient to be implemented in MANETs.As in this proposed system there is slight increase in the routing overhead, so in future, to enhance the performance of the mobile ad hoc networks more effectively, the main area of research will going to be concentrated on adaptation of hybrid cryptographic techniques to reduce the network overhead.Also the implementation of this system in real time environment and making analysis from obtained results is one of the main concerns in future work.

7. REFERENCES

[1] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks,"*Symposium on Applications and the Internet Workshops* IEEE, pp. 368-373, 2003.

[2] A. Nadeem and M. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks,"2013.

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

[4] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf.Perform., Comput., Commun.,*pp. 747–752, 2004.

[5] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "Anacknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[6] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", *in proc. 24th IEEE International Conference on Advanced Information Networking and Applications,*pp. 635-640, 2010.

[7] Qasim M Alriyami, Eleana Asimakopoulou, Nik Bessis "A Survey of Intrusion Detection Systems for Mobile Ad-Hoc Networks", *in proc. IEEE, International Conference on Intelligent Networking and Collaborative Systems*, 2014.

[8] Sara CHADLI, Mohamed EMHARRAF, Mohammed SABER, Abdelhak ZIYYAT, "Combination of hierarchical and cooperative models of an IDS for MANETs*"in proc. IEEE Tenth International Conference on Signal-Image Technology & Internet-Based Systems*, pp. 230-236, 2014.

[9] Akshatha Y., Dr. Rashmi M. Jogdand, "Enhanced Adaptive Acknowledgement Method for detecting Malicious Nodes in MANET", *IOSR journal of Computer Engineering*, vol. 16, Issue 4, ver. I, pp 32-38, 2014.

[10] Digital signature, URL: http://cr.yp.to/ecdh.html