Enhanced Adaptive Acknowledgements for MANETs by using a Secure Intrusion Detection System

Vibha U
M.Tech Student, Department of CSE,
SEA College of Engineering and Technology,
Bangalore- 560049

Dr. B. R. Prasad Babu
Professor and Head, Departement of CSE , R & D Center,
SEA College of Engineering and Technology,
Bangalore – 560049

Mrs. Jayashri. M
Asst Professor,Department of CSE,
SEA College of Engineering and Technology,
Bangalore – 560049

***Abstract* - In the past few decades the transmission from wired network to wired network has been a global trend. Many applications have been made possible by wireless network due to the scalability and mobility. There is no fixed network infrastructure for MANETs; every node act as both a transmitter and receiver .Nodes communicates directly when they are within the same range of communication. Otherwise, they depend on their neighbors to transmit messages. The Configuring ability of nodes in MANET is safe so that it is made popular among critical applications like military use or emergency recovery. Security is very important service in Mobile Ad hoc Network. MANETs are more susceptible to various types of attacks. Here is a new IDS named Enhanced Adaptive ACKnowledgement (EAACK) which is specially designed for MANETs.**

Keywords - Enhanced Adaptive ACKnowledgement (EAACK), Mobile Ad hoc NETwork (MANET), Intrusion Detection System (IDS), Dynamic Source Routing(DSR)

I. INTRODUCTION

A collection of wireless mobile hosts (or nodes) that are equipped with a wireless transmitter and a receiver that communicate directly with each other or forward message through other hosts is said to be a Mobile Ad hoc Network(MANET).One of the major advantages of mobile networks is that it allows different nodes for data communication and still maintains their mobility. But, this communication is very much limited to the range of transmitters. It means that when the two hosts distance is beyond the range of communication of their own then that two hosts cannot communicate. MANET solves this problem by allowing neighboring nodes to rely data transmissions. By dividing MANET into two types of networks such as single-hop and multi-hop [13] this can be achieved. In the single-hop network, all nodes will be in a same communication range and they directly communicate with each other. But in multi-hop, nodes rely on other neighboring nodes to transmit if the nodes are not in the same communication range [1]. Self-organizing and self-managing network without the support of any fixed infrastructure is one of the advantages of MANETs. An expensive base station of infrastructure dependent network is not required for MANETs. Since MANET is being used in a wide spread, security has become a very important issu[2]. The mechanism that performs the task of security to MANETs is called Intrusion Detection system (IDS)[2][3].

.

II. RELATED WORK

A. IDS in MANETs

Intrusion detection is a type of security management system for computers and network. For MANETs the general function of IDS is to detect misbehaviors by observing the networks traffic. There are two important models of Intrusion Detection systems namely: signature based and anomaly based approaches [5][6]. A signature-based IDS monitors activities on the networks and compares them with known attacks. However drawback of this approach is that new unknown threats cannot be detected. In anomaly-based approach, profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically and significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, but the issue is that anomaly based approaches yield high false positives for a wired network. If these statistical approaches are applied to MANET, the false positive problem will be worse because of the unpredictable topology changes due to node mobility in MANETs. The specification-based approach is recently presented and is ideal for new environments such as MANETs. In case of specification-based detection, the behavior of critical objects that are correct will be taken and will be made as security specifications, which are compared to the actual behaviors of the exact knowledge about the nature of the intrusions. Currently, specification-based detection has been applied to privileged programs, applications, and several network protocols. Security is most important service in MANETs.

B. Security attributes

Security has become a very much important service in Mobile Ad hoc Network [12]. To secure an ad hoc network, the following attributes are to be considered: availability, authentication and key management, confidentiality, integrity, non-repudiation and scalability. In order to achieve this goal, the security solutions for each layer which are providing complete protection for MANETs are to be described.

There are five main layers on the network as follows:
1. Application layer: Detecting and preventing viruses, worms, malicious codes.

2. Transport layer: Authenticating an securing end-to-end communication through data encryption.
3. Network layer: Protecting the ad hoc routing and forwarding protocols.

4. Link layer: Protecting the wireless MAC protocol and providing link-layer security support.

5. Physical layer: Preventing signal jamming denial-of-service attacks.

C. Discovering malicious nodes

1. Watchdog: It is an IDS for improving the throughput of network. Watchdog IDS can be classified into two methods such as Watchdog and Path rater. It is responsible for discovering malicious node misbehaviors in the network. If a watchdog IDS overhears that its next coming node unable to forward the packet within a certain period of time, failure counter will be increased. Whenever a individual node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as a misbehaving node. In such a case, the Path rater cooperates to avoid the future transmission of packets.

The Watchdog scheme fails to detect the malicious misbehaviors with the presence of following: 1)ambiguous collisions; 2)receiver collisions; 3)limited transmission power; 4)false misbehavior report; 5)collusion and 6)partial dropping.

2. TWOACK: TWOACK is neither an enhanced nor a Watchdog-based scheme. TWOACK Aims to resolve the problems of Watchdog such as limited transmission power and receiver collision. It detects misbehaving links but acknowledging every data packet transmitted over every three consecutive nodes along the path from source to the destination. Each node is required to send back an acknowledgement packet to the node that is two hops away from it in the same route but in reverse order.

The TWOACK IDS processes the problems of watchdog such as limited transmission power and receiver collision. But, the acknowledgement is required for every packet transmission process, so that the unwanted network overhead may araise. As battery power of MANETs is limited, the life span of the network may degrade early.

3. AACK: AACK can be considered as a combination of a scheme called TWOACK and Acknowledgement (ACK). AACK significantly reduces network overhead and also it is capable of maintaining the network throughput.

III. PROPOSED SYSTEM

Secure IDS architecture(EAACK) introduced to improve the security level of MANETs based on security attributes and various algorithm namely, RSA and DSA.EAACK is designed to tackle three out of six weaknesses of Watchdog IDS, namely,
1) Receiver collision
2) Limited transmission power
3) False misbehavior.

1. **Receiver collision**: Here the below figure1 shows the example of receiver collision. Here node A sends Packet 1 to node B and node A tries to overhears that node C received the packet which has been forwarded by node B. At the same time, Packet 2 is also forwarded by node X to node C. In such case, node C cannot receive any of the packets due to a collision at node C between the packet 1 and 2.

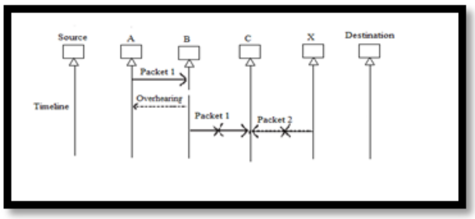

Figure1. Receiver collision: Here two nodes B and X both sends the Packet 1 and Packet 2 respectively to node C at the same time.

2. Limited transmission: In limited transmission power, every node will be having the limited transmission power in order to preserve the battery resources of its own. Example for limited transmission is shown below in figure 2. Here node B limits its transmission power intentionally but the node A overhears that packet 1 has been transmitted to node C but node B fails to transmit the packet to node C as it is having limited power of transmission. So that it is node B cannot be able to transmit the packet to node C.

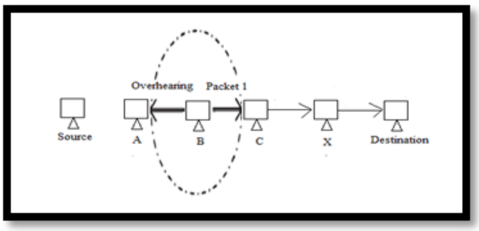

Figure2. Limited transmission power: Here Node B limits its power of transmission so that it cannot transmit the packet 1 to node C. But node A overhears that packet 1 has been transmitted to node C.

3.False misbehavior: Example of false misbehavior in MANETs, shown in fig 3. Here node A successfully overhears that node B forwarded Packet 1 to node C, but still node A reports node B as misbehaving. This is because of open medium and remote distribution of MANETs, any attackers can easily achieve this false misbehavior report by capturing one or more nodes..

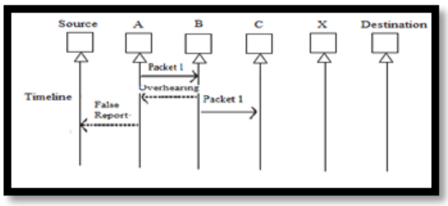

Figure3. False misbehavior report: Here Node A sends back a misbehavior report to source even though node C receieved the packets 1 from node B.

As discussed earlier, TWOACK and AACk solve two weaknesses namely, receiver collision and limited transmission power of watchdog. However, both of them are sensible to the false misbehavior attack. Here we propose new IDS which solves not only receiver collision and limited transmission power but also the false misbehavior problem for MANETs.

Furthermore, we extend to adopt a digital signature scheme during the packet transmission process in order to get the acknowledgement of packet transmission from the individual nodes.

IV. SCHEME DESCRIPTION

EAACK consist of three major parts namely, ACK, secure ACK(S-ACK) and misbehavior report authentication (MRA).

A. ACK

ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Here the source node S first sends a data packet to the destination node D. If all the intermediate nodes cooperate for transmission of packets to node D from node S then node D successfully receives packet. After receiving the packet node D has to send back an ACK acknowledgement packet in the same route but in a reverse order. Within a predefined period, node S has to receive an acknowledgement from node D if packet has been received by node D successfully. Otherwise, node S will switch to S-ACK mode to detect the misbehaving nodes in the route by sending out an S-ACK data packet.

B. S-ACK

S-ACK is an improved version of TWOACK IDS[6]. Here also every three consecutive nodes work to detect misbehaving nodes. Here every three consecutive nodes in the route that is the every third nodes are required to send an S-ACK to the source to detect misbehaving nodes. But this S-ACK mode will not be aware of receiver collision or limited transmission power.

C. MRA

MRA mode will get activated when the S-ACK mode reports the misbehaving node. This mode will get activated in order to check whether the report is correct or not. In order to initiate MRA node, first source node searches for an alternative path to the destination. In order to search an alternative path, source node starts a DSR routing request to find another path to the destination. By using alternative path source node sends the MRA-packet to the destination. If the packet sent by source is already present and if it matches the packet sent by S-ACK mode in the destination then it can be concluded as the report is false misbehavior report. Otherwise, the report sent by S-ACK mode will be trusted and accepted.

V.CONCLUSION

Packet-dropping attack has always been a major threat to security in MANETs. A Secure Intrusion-Detection by Enhanced Adaptive Acknowledgement protocols specially designed for MANETs solves the problem of limited transmission power, receiver collision and false misbehavior report. We conclude that this scheme is very useful when security in the network is the top priority.

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] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad,2009."Chapter 30:Security in wireless ad- hoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publisher

[4] 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.

[6] 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.

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