IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 14-18
www.iosrjournals.org

Comparative Study of Ids for Manet

R Ranjani[1], JJayalakshmi[2]
[1]*PG Scholar, Dept. of Electronics and CommunicationEngg, Saveetha Engineering College, India*
[2]*Assoc. Prof., Dept. of Electronics and CommunicationEngg, Saveetha Engineering College, India*

Abstract: *Recent advancements in wireless communication and the miniaturization of computers have led to a new concept called the mobile ad hoc network (MANET), where two or more mobile nodes can form a temporary network without need of any existing network infrastructure or centralized administration. Even if the source and the destination mobile hosts are not in the communication range of each other, data packets are forwarded to the destination mobile host by relaying the transmission through other mobile hosts which exist between the two mobile hosts. Since no special infrastructure is required, in various fields such as military and rescue affairs, many applications are expected to be developed for ad hoc networks. Nevertheless, the exposed medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this situation, it is necessary to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Since MANETs is used in many applications it isnecessary to provide more security. In this paper, we suggest and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) with cluster based communicationspecifically designed for MANETs. Compared to current approaches, EAACK with cluster based communication demonstrates higher malicious-behavior-detection rates in certain environments.*

Keywords:*Digital signature, EAACK, Intrusion Detection System, Mobile Ad hoc Network (MANET), Security.*

I. Introduction

A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices linked by wireless. Each node in a MANET is free to move freely in any direction, and will consequently change its links to other devices frequently. The main challenge in constructing a MANET is providing each device to continuously maintain the information required to accurately route traffic. Networks may work by themselves or may be connected to the moreInternets. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. In manet each node may function as both host and a router. Since there is no fixed network the control and management operations are distributed among the terminals. It has multi-hop routing; packets should be delivered via one or more nodes.

A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battle field and there is no infrastructure to help them form a network [1]. In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, extending from military to civilian and marketable uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Hence, only one compromised node in the network can cause the failure of the entire network.

II. Related Work

Intrusion Detection Systems which is used to detect and report the malicious activity in ad hoc networks. IDS look for attack signatures, which are specific configurations that frequently indicate malicious or suspicious intent. Nodes in MANETs assume that other nodes always cooperate with each other to transmit data. This statement leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To discoursethis difficult, an IDS should be added to improve the security level of MANETs. The first assumption is that before the attackers entering the network, if it detected, then we will be able to completely abolish the probableharms caused by negotiated nodes. In this section, we mainly describe three existing methodologies, namely, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK) [2] [4] [5].

1) Watchdog: The goal of Watchdog is to improve the throughput of network withthe presence of malicious nodes. In fact, two techniques were introduced in Watchdog scheme, namely, Watchdog and Pathrater. The Watchdog technique identifies the misbehaving nodes by overhearing in the network. The malicious misbehaviors in the network are detected by listening to its next hop's transmission. Watchdog node sets a period of time for the node, which is ready to forward the packet to the next node. If that node fails to

forward the packet within that time, then it is overheard by the Watchdog node and it increases the failure counter of that node. Whenever a node's failure counter exceeds analready decided threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme However,the Watchdog scheme fails to detect malicious misbehaviors with the presenceof the following: 1) receiver collisions;2) limited transmission power; 3) false misbehavior report; 4) partial dropping.

2) TWOACK: The TWOACK scheme is to moderate the opposing effects of misbehaving nodes. The basic idea of the TWOACK scheme is that, when a node sends a data packet successfully over the following hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called TWOACK to indicate that the data packet has been received successfully [3]. Such a TWOACK transmission takes place for only a fraction of data packets, but not all. Such a "selective" acknowledgment is intended to reduce the additional routing overhead caused by the TWOACK scheme. Upon recovery of a packet, every node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. However, the acknowledgment process required in every packet transmission process added a significant amount of undesirable network overhead. Due to the restricted battery powernature of MANETs, such terminated transmission process can easily destroy the life span of the entire network.

3) AACK: Adaptive ACKnowledgment (AACK), for solving two significant problems: the limited transmission power and receiver collision. TheAACK scheme is an enhancement to the TWOACK scheme where its detection overhead is reduced while the detection efficiency is increased. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered 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 significantly reduced network overhead while still capable of maintaining or even surpassing the samenetwork throughput.

III. Proposed System

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA).In EAACK protocol, we focused on solving these four possible attacks to watchdog scheme. With the introduction of DSA to our scheme, we can further extend it to be able to detect contaminated messages as well. Due to the nature of wireless transmission, man-in-the-middle attack can be easily achieved as signals are being broadcast over the air. Attackers can easily capture one packet and modify it with malicious payload [6].

A. ACK

ACK is basically an end-to-end acknowledgment based scheme. It performs as a part of the hybrid scheme in EAACK, pointing to decrease network overhead when no network misbehaviour is detected. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet [7].

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. In a network, for every three consecutive nodes in the route, the third node in the route is required to send an S-ACK acknowledgment packet to the first node in the route. The purpose of presenting S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.However, unlike the TWOACK scheme, where the source node directly trusts the misbehavior report, EAACK with cluster requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

D. Digital Signature

Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature.

EAACK with cluster is an acknowledgment-based Intrusion Detection System. The three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection techniques. They all trust on acknowledgment packets to detect misbehaviors in the network. Thus, it is particularly important to ensure that all acknowledgment packets in EAACK are authentic and uncorrupted. Or else, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes of EAACK with cluster will be susceptible to the attackers. With regard to this urgent concern, we integrated digital signature in our proposed scheme. In order to safeguard the integrity of the IDS, EAACK with cluster requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. Nevertheless, we fully understand the extra resources that are required with the introduction ofdigital signature in MANETs. The goal is to find the most optimal solution for using digital signature in MANETs.

E. Cluster Communication

To further improve the security level, we include a cluster based communication in manet. Clustering is a technique to group nodes in a network into separating or overlapping entities called clusters. The clustering structure divides a network into one or several clusters, one of which consists of one cluster head and some cluster members. However, in a clustering network the cluster head serves as a local coordinator for its cluster, performing inter-cluster routing, data forwarding. In particular, cluster based communication also maintains the scalability and energy efficiency. EAACK is based on ACK, S-ACK, and MRA. Instead of using ACK scheme we can also implement through TWOACK scheme [3]. The information about the cluster nodes will be available in the cluster head. So the malicious node can be easily identified by the neighboring nodes and the cluster head. Whenever data transmission takes place, the cluster head will not include the malicious node for the transmission and transmits packets through other nodes. Further we cannot completely remove the malicious node in the wireless network, instead we can avoid the malicious node during the transmission.

IV. Performance Evaluation

In this section, we will describe our simulation environmentand compare our simulation result with Watchdog, TWOACK, AACK and EAACK schemes.

A. Simulation Parameters

In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B.

Table 1. Simulation parameters for the multicast

No. of Nodes	50
Speed of Node	20 m/s
Area Size	670 X 670 m
Mac	802.11
Simulation Time	50 sec
Traffic Source	CBR
Transmission Rate	250m
Routing Protocol	AODV

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. In order to compare the performances of our proposed scheme, we continue to implement the following twoperformance metrics.

1) *Packet delivery ratio (PDR)*: Packet Delivery Ratio defines the ratio of the total number of packets received by the destination node to the total number of packets sent by the source node.

2) *Routing overhead (RO)*: RO defines the ratio of theamount of routing-related transmissions.

To pretend the malicious nodes, we adapted the network simulator to let certain amount of nodes behaves like malicious nodes. However, when being requested to forward a data packet, they will drop the data packet and send a forged acknowledgement packet whenever possible. By doing this, we simulate the smart attackers who try to drop the data packets without being detected.

C. Simulation and Analysis

Here we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. Thissetting is designed to test the IDS's performance under the false misbehavior report.

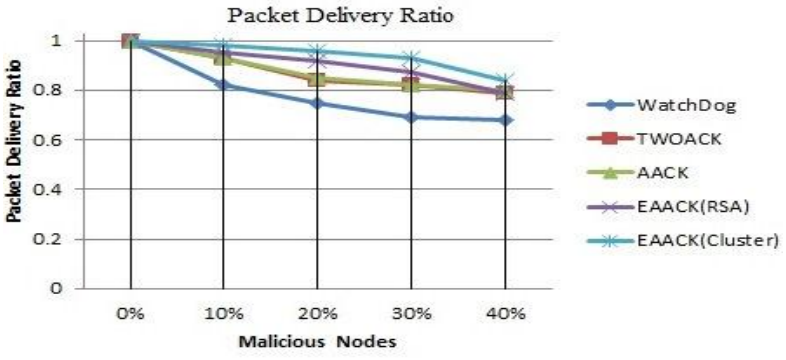

Fig. 1. Packet Delivery Ratio

Fig. 1.shows the achieved simulation results based on PDR. When malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report. By introducing cluster based communication in EAACK, security is further improved in manet. The above simulation result compares the performance of the Intrusion Detection Systems. And it proves that EAACK with Cluster Based Communication is more secure than the other existing Intrusion Detection system

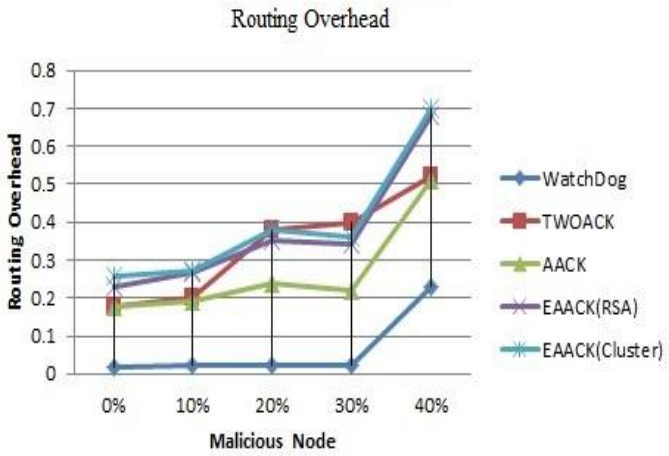

Fig. 2. Routing Overhead

In terms of RO, owing to the scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, as shown in Fig. 2. However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more malicious nodes require a lot more acknowledgment packets and digital signatures.

V. Conclusion

Packet-dropping attack has always been a major threat to the security in MANETs. The existing Intrusion detection system named Watchdog, TWOACK, and AACK Schemes are simulated using NS2 and the disadvantages of the existing approaches are the receiver collision, limited transmission power, false misbehavior report, partial dropping. A new intrusion detection system named EAACK with cluster based communication specially designed for MANETs and the performance of EAACK is compared with the other popular mechanisms through simulations. The simulation results are compared against in the cases of receiver collision, limited transmission power, and false misbehavior report of the existing mechanisms. The digital signature is incorporated to prevent the attackers from initiating forged acknowledgment attacks. Furthermore, a cluster communication is introduced in the proposed scheme to improve the performance of the packet delivery ratio.

References

[1]. R. H. Akbani, S. Patel, and D. C. Jinwala,"DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012,pp. 535–541.

[2]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008,.

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

[4]. N. Nasser and Y. Chen,"Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int.Conf. Commun.*, Glasgow, Scotland, 2007,pp. 1154–1159.

[5]. 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.*, 2004,pp. 747–752.

[6]. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE Trans. Ind Electron.,2013, Vol. 60, no. 3.

[7]. A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis,"Secure routing and intrusion detection in ad hoc networks," in *Proc. 3rd Int. Conf.Pervasive Comput. Commun.*,2005,pp. 191–199.