e-ISSN : 2349-9745
p-ISSN : 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Malicious Detection in MANET Using Enhanced Adaptive Acknowledgement

Vinodhini.C[1],Sakthivel.S[2]
[1]*Dept of ECE, Vivekanandha college of engineering for women*
[2]*Assistant professor, Dept of ECE, Vivekanandha college of engineering for women*

Abstract-- Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. Node works as both transmitter and a receiver and in which MANET does not require a fixed network infrastructure.Within the communication range,the nodes can communicate with each other.MANET made popular in military use and emergency recovery.In this paper a new approach for intrusion and detection system named EEACK is proposed. Both of the TWOACK and Watchdog methods are considered as the first line of defense and it is not sufficient to protect MANETs from packet dropping attacks. EAACK provide higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. This paper proposes a mechanism for a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations and migration to wireless network from wired network.

Keywords--Digital signature,digital signature algorithm(DSA),Enhanced Adaptive ACKnowledgment (AACK) (EAACK),Mobile Ad hoc NETwork (MANET).

I. INTRODUCTION

A mobile ad hoc network (MANET) is a one of the wireless method. The devices are moving in randomly different directions and communicating with one to another within each nodes communication range. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly.Wireless network allows data Communication between different parties.MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes communicate directly with each other nodes within the same radio range.In a multihop node forward a packet to a node that is out of its radio range,to the cooperation of other nodes in the network is known as multi-hop communication.An intrusion-detection system (IDS) specially designed for MANETs.IDS can be defined as a process of monitoring activities in a system,which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS).

II. RELATED WORKS

2.1.WATCHDOG:

Watchdog serves as an IDS for MANETs.Watchdog is used for detecting malicious node misbehaviour in the network. The Watchdog scheme is consisted of two parts namely, Watchdog and Path rater. Watchdog node reports it as misbehaving and the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission.[1]If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Watchdog is capable of detecting malicious nodes rather than links.

2.2 TWOACK:

TWOACK is neither an enhancement nor a Watchdog-based scheme and it is one of the most important approaches among IDS method . Aiming to resolve the receiver collision and limited transmission power problems 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.In TWOACK Each node is required to send back an acknowledgment
packet to the node that is two hops away from it.

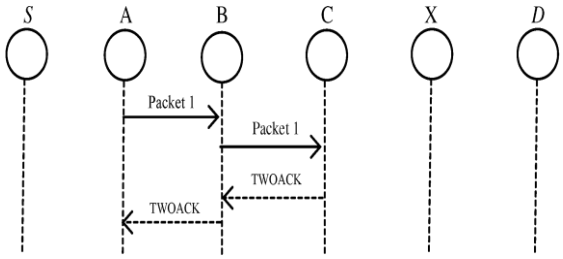


FIGURE.1 TWOACK

2.3 AACK:

Based on TWOACK proposed a new scheme called as AACK. ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK. In AACK mode, node S first sends out an ACK data packet Packet1 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 Packet1, node D is required to send back an ACK acknowledgment packet Packet1 along the same route but in a reverse order.

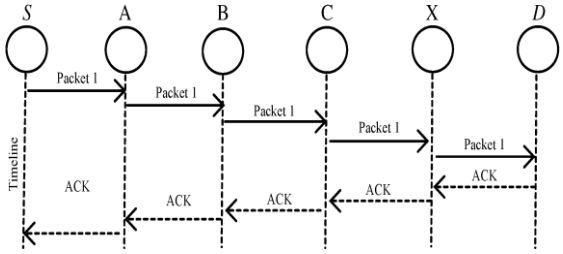


FIGURE.2 AACK

III. DIGITAL SIGNATURE

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs.

Digital signature schemes can be mainly divided into thefollowing two categories.

1) *Digital signature with appendix*:The original message is required in the signature verification algorithm. Examples include a digital signature algorithm.

2) *Digital signature with message recovery*: This type of scheme does not require any other.

Information besides the signature itself in the verification process.

First, a fixed-length message digest is computed through a preagreed hash function H for every message m. This process can be described as

$$H(m) = d.$$

Second, the sender Alice needs to apply its own private key *Pr−Alice* on the computed message digest *d*. The result is a signature *Sig*Alice, which is attached to message *m* and Alice's secret private key

$$SPr-Alice\ (d) = Sig\text{Alice}. \quad (2)$$

To ensure the validity of the digital signature, the sende Alice is obliged to always keep her private key *Pr−Alice* as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob[2]. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages.from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.Next, Alice can send a message *m* along with the signature *Sig* Alice to Bob via an unsecured channel. Bob then computes the received message *m*_ against the preagreed hash function *H* to get the message digest d .

$$H(m) = d$$

IV. PROPOSED SYSTEM

We propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances we implemented both DSA and RSA in our proposed EAACK scheme. The main purpose of this implementation is to compare their performances in MANETs. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

4.1 EEACK:

A new intrusion-detection system named Enhanced Adaptive ACKnowledgment(EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances[3]**.** EAACK is consisted of three major parts, namely, ACK,secure ACK (S-ACK), and misbehavior report authentication(MRA).

4.2 ACK:

In ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D.If all the intermediate nodes along the route between nodes Sand D are cooperative and node D successfully receives *Pad*1,node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, 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. The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

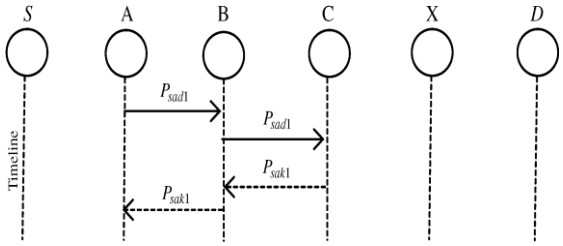


FIGURE 3. ACK scheme

4.3 SECURE-ACKNOWLEDGMENT

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al*. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes[4]. 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 intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

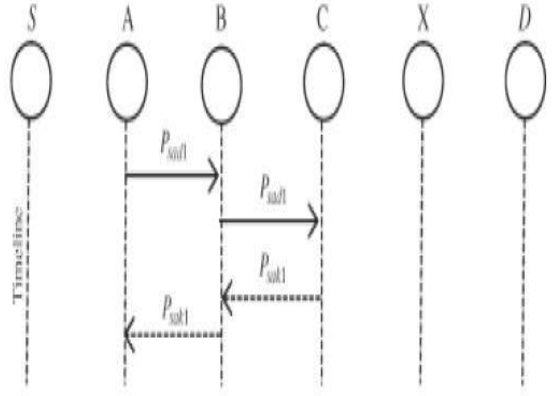


FIGURE 4. S-ACK

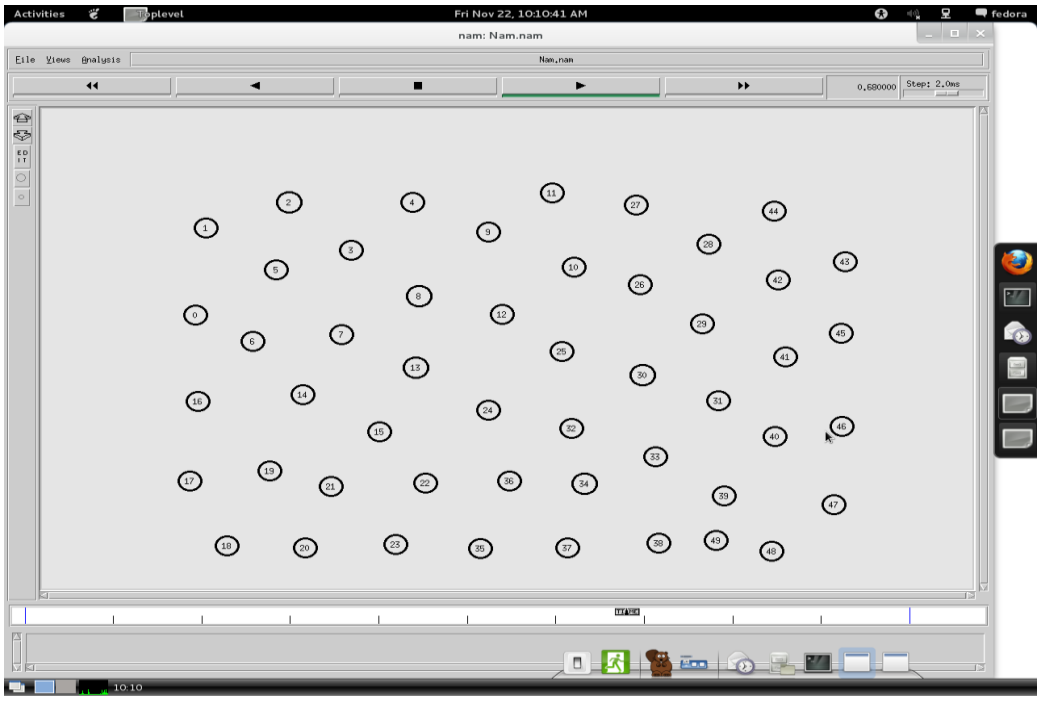
4.4 MRA

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 misbehavior 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[5]. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious. Or else, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. Since discussed earlier, All three parts of EAACK, that is, ACK, S-ACK, and MRA, are acknowledgment-based detection scheme. They all rely on response packets to discover misbehaviors in the network.

Hence, it is really important to ensure to everyone acknowledgment packets in EAACK are authentic and untainted. If not, if the attackers are smart sufficient to forge acknowledgment packets, all of the three schemes will be vulnerable. However, we fully understand the extra resources that are required with the beginning of digital signature in MANETs. To address this concern, we implemented both DSA [6] and RSA digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

4.5 SIMULATION RESULTS



V. CONCLUSION

In MANET Packet-dropping attack has been a major threat we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations.this paper positive performances against Watchdog,TWOACK, and AACK.In our future research, To avoid or minimize partial Packet-dropping in misbehavior in network communication and Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys.

REFERENCES

[1]Elhadi M.Shakshuki,Senior Member,IEEE,Nan Kang, and Tarek R.Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs"IEEETrans.Ind.Electron..,Vol 60.No. 3,March 2013.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc NetworkSecurity," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

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

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

[5] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10,2010, pp. 216–222.

[6] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*,vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

