ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Performance Analysis for Manet Using Secured Algorithm

A.Vijayalakshmi[1]

M.E communication systems, K. Ramakrishnan College of Engineering, Trichy, India. [1]

ABSTRACT— Mobile Ad hoc Network (MANET) is a collection of mobile nodes that communicate with each other. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. To protect from attacks they developed Intrusion detection system of Enhanced adaptive acknowledgement it leads to network overhead. The proposed scheme is AUTOSAR algorithm is used to overcome the enhanced adaptive Acknowledgement problem. It improves the performance metrics.

KEYWORDS—EAACK, ACK, S-ACK, Digital signature

I. INTRODUCTION

Due to the mobility and scalability, wireless networks are always preferred. Due to the improved technology and reduced costs, wireless networks preference over wired networks in the past few decades. Mobile Ad-hoc Network (MANET) is a collection of mobile nodes operational with both a wireless transmitter and a receiver that communicate with each other through bidirectional wireless links either directly or in some way. Industrial remote access and control through wireless networks are fitting. Advantages of wireless networks are ability to allow data communication between different parties and maintain their mobility. Communication is limited to the range of transmitters. Two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Furthermore, because of MANETs distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. BACKGROUND

A. Intrusion detection system in MANET

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches; mainly describe three existing approaches, specifically Watchdog scheme, TWOACK and Adaptive ACKnowledgment (AACK).

1. Watchdog scheme

Watchdog scheme that aims to improve the throughput of network with the presence of malicious nodes. The Watchdog scheme is consisted of two parts namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is conscientious for detecting malicious node misbehaviors in the network.Watchdog detect malicious misbehaviors by listening to its next hop's transmission. 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. Every time a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this crate, the Pathrater cooperate with the routing protocols to avoid the reported nodes in future transmission.

2. Two Acknowledgement scheme

TWOACK is neither an enhancement nor a Watchdog-based scheme. aim 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. Upon rescue of a packet, each 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. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is shown in Fig. 1 Node A first forwards Packet 1 to node B and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is indebted to create a TWOACK packet which contains reverse route from node A to node C and sends it back to node A. The recovery of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. or else, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same procedure applies to every three uninterrupted nodes along the respite of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems by watchdog.

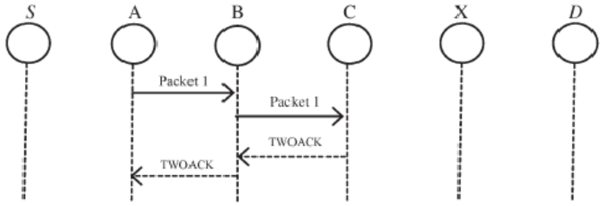

Fig. 1 TWOACK Scheme

However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

3. Adaptive Acknowledgement scheme

AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called 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 same network throughput.

In the ACK scheme is shown in Fig. 2, the source node S sends out Packet 1 without any overhead except of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out a TWOACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

4. 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. The development of cryptography technique has a long and fascinating history. Digital signature schemes can be mainly divided into the following two categories.

1) The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).
2) Another scheme does not require any other information besides the signature itself in the verification process. Examples include RSA. The general flow of data communication with digital signature. First, a fixed-length message digest is computed through a pre agreed hash function H for every message m. This process can be described as

$$H(m) = d \qquad (3.1)$$

Second, the sender Alice desires to apply its own private key $P_{r\text{-}Alice}$ on the compute message digest d. The result is a signature Sig_{Alice}, which is attached to message m and Alice's secret private key

$$S_{\text{Pr-Alice}} = Sig_{Alice} \qquad (3.2)$$

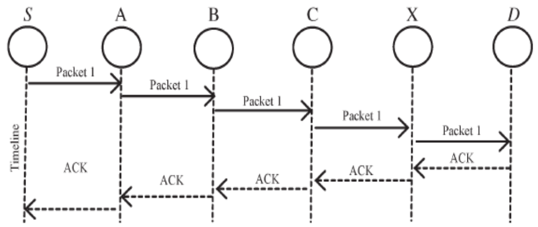

Fig. 2 ACK Scheme

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $P_{r\text{-}Alice}$ 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. 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 against the pre agreed hash function H to get the message digest d'. This process can be generalized as

$$H(m')=d' \qquad (3.3)$$

Bob can verify the signature by applying Alice's public key $P_{r\text{-}Alice}$ on Sig_{Alice}, by using

$$S_{\text{Pr-Alice}}(Sig_{Alice}) = d. \qquad (3.4)$$

If $d == d'$, then it is safe to claim that the message m' transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

B. *Problem identification*

The proposed approach EAACK is designed to tackle weaknesses of Watchdog scheme namely, false misbehavior, limited transmission power, and receiver collision. Example of receiver collisions is shown in Fig. 3, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

Example of limited transmission power is shown in Fig. 4, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C.Example of false misbehavior report is shown in Fig. 5, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving

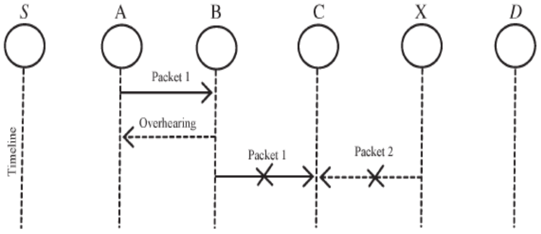

Fig. 3 Receiver collision

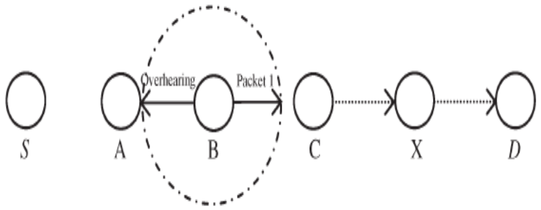

Fig. 4 Limited transmission power

Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

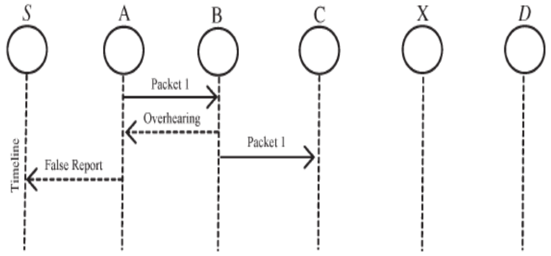

Fig. 5 False misbehavior report

C. *Proposed system*

EAACK is the Enhanced adaptive acknowledgement consisted of three major parts, namely ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).According to the Internet draft of DSR, there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. The link between each node in the network is bidirectional. For each communication process, both the source node and the destination node are not malicious Unless specified, all acknowledgment packets described are required to be digitally signed by its sender and verified by its receiver. System control flow of EAACK scheme.

1. Acknowledgement scheme

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metric packet delivery ratio defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. RO defines the ratio of the amount of routing related transmissions.

If all the intermediate nodes along the route between nodes S and 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.

2. Secure Acknowledgement scheme

The aim of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *Psad*1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives *Psad*1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 forwards *Psak*1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.

3. Misbehavior report authentication

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. The interior of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To commence 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.

4. Digital signature

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is a great deal important to ensure that all acknowledgment packets in EAACK are authentic. Or else, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be susceptible. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and confirmed in anticipation of they are established.

D. Performance evaluation

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performances metric. *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. *Routing overhead (RO)* defines the ratio of the amount of routing-related transmissions [Route Request (RREQ), Route Reply (RREP), Route Error (RERR), ACK, S-ACK, and MRA].

III. SIMULATION RESULTS

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metric packet delivery ratios defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. RO defines the ratio of the amount of routing related transmissions.

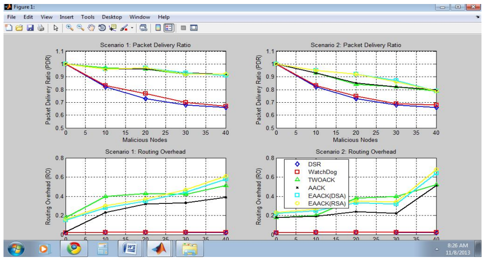

Fig. 8 Performance evaluation of scenario 1 and 2

The above fig.8 shows the performance evaluation of DSR, Watchdog, Twoack, AACK, EAACK (DSA), and EAACK (RSA). The graph shows the packet delivery ratio and routing overhead in two different scenarios.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

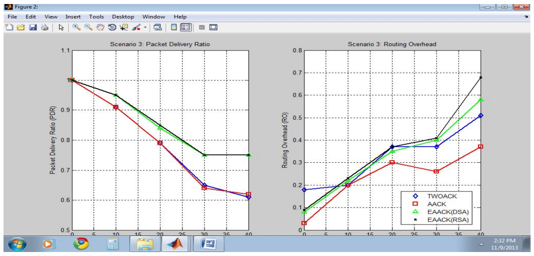

Fig. 9 Performance evaluation of scenario 3

The fig.9 shows the packet delivery ratio and routing overhead in third scenario. In all the three scenarios EAACK DSA and EAACK RSA gives best performance. But in terms of computational power EAACK DSA is preferable.

IV. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. EAACK protocol specially designed for MANETs is proposed and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. To prevent the attackers from initiating forged acknowledgment attacks extended to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. In order to seek the optimal DSA in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits of research work, plan to investigate the following issues in future research possibilities of adopting AUTOSAR techniques to further reduce the network overhead caused by digital signature, and improving the performance metrics.

V. REFERENCES

[1] Bo Sun And Lawrence Osborne, Lama University Yang Xiao, "Intrusion Detection Techniques In Mobile Ad Hoc And Wireless Sensor Networks", IEEE Wireless Communications October 2007.

[2] David B. Johnson David A. Maltz, "Dynamic Source Routing", IEEE Transaction on Networks,november/december 1996.

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

[4] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol-A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.

[5] K. Kuladinith, A. S. Timm-Giel, and C. Gorg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323,2004.

[6] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE Transaction on Networks,november/december 1999.