ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

A novel approach Using acknowledgement for highly efficient secured intrusion -detection system for MANETS

Kavyashree G M

M.Tech, Computer Networks, Sridevi Institute of Technology, Kenjar, Mangalore, India

Abstract: A wireless network is method by which homes, telecommunications network and business enterprise installations, avoid the costly process of introducing the cables or connection between various equipment locations. Mobile ad hoc networks are an infrastructure less internet protocol based network. The absence of centralized firewall and distributed nature of operation of nodes make MANETS vulnerable to malicious attacks. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, it is vital to address its potential security issues. In this paper, 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.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Network (MANET).

I. INTRODUCTION

MANETs are the mobile adhoc networks consist of collection of nodes, includes both transmitter and receiver. Nodes are communicating bidirectional via wireless networks. MANETs have ability to allow data communication between different parties. Due to their ability and scalability of wireless networks improved technology reduces the cost of wireless networks. The converse of wired networks, wireless networks is ability to allow the data communication between the different parties and maintain mobility. However, the lack of communication range two nodes cannot communicate with each other. This is the one of the main issue in the wireless networks. MANETs will provide a solution, in the way of allowing the intermediate parties between the nodes. Each nodes relay on their intermediate node to transmit, if the destination node is out of the communication range.

MANETs does not require fixed infrastructure. All the nodes are free to move randomly [1]. Because of this self configuring nature ability to create a centralized infrastructure. The quick configuration make the MANETs are efficient use in emergency circumstances, where infrastructure is unavailable [1][2]. The above characteristics of MANETs have widely implemented in several areas. The main issue is that the nodes present in the network are having lack of physical security. There is no guarantee about packet transmission between the nodes. Because of this scenario the attackers can easily compromise with the nodes present in the network. The dynamic distribution and co-operative nature of the nodes the attackers can easily inert the malicious nodes into the network. Centralized monitoring technique can also no longer feasible in MANETs. In such a criteria important to develop an intrusion detection system (IDS). this technique provide a security to the each nodes , and it is especially designed for the MANETs type of networks.

II. BACKGROUND

As discussed before, all nodes in a MANETs are relay the data to communicate with each node. The range of communication is also depends upon the transmission ability of the nodes and also the battery power. Due to such limitations the attackers have significant opportunities to achieve their impact with one or two compromised nodes. IDS provide a proactive approach to the existing system. It will eliminate the potential damages caused by compromised nodes and enhance the security level of MANETs.

In this section mainly describe three existing approaches namely, watchdog [7], TWOACK [6], AACK [9]. *1) Watchdog:* This technique describe the two technique improve the throughput in an adhoc network in the presence of the nodes they agree to forward the packet but fail to do so. This technique categorizing the nodes based upon the dynamically measured behavior. Watchdog and path rater are the main technique, identifies the misbehaving nodes and helps the routing protocols. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) Ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. 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. Upon retrieval 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. The working process of TWOACK is shown in Fig. 1.

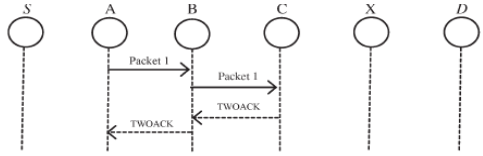

Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. 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) AACK: 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). The end-to-end acknowledgment scheme in ACK is shown in Fig. 2.

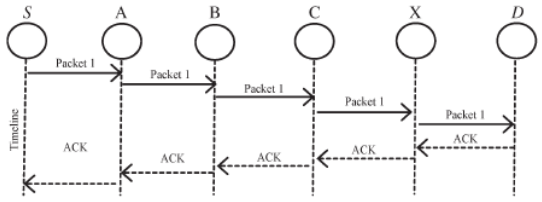

Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

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 TACK scheme by sending out a TACK 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. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

III. PROBLEM DEFINITION

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses in detail. In a typical example of receiver collisions, 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 Packet1and Packet2 at node C.

In the case of limited transmission power, 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, as shown in Fig. 4.

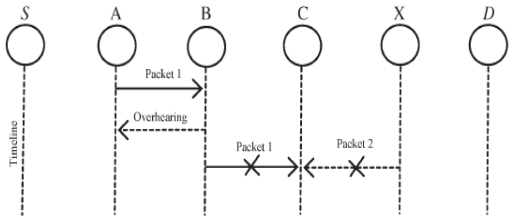

Fig3. Receiver Collision: both node B and X are trying to send packets1 and packet 2 respectively, to node c at the same time.

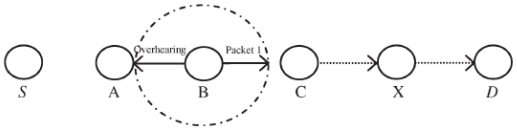

Fig4. Limited transmission power: node B limits the transmission power so that packet transmission can be overhead by node A but too weak to each node C.

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving, as shown in Fig. 5. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one sor two nodes to achieve this false misbehavior report attack.

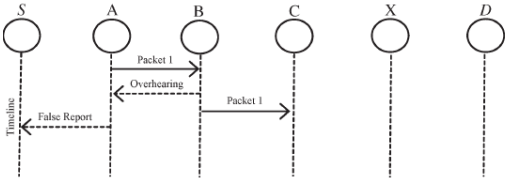

Fig5. False misbehavior report. Node A sends back misbehavior report even through the node B forward the packet to node C.

As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

collision and limited transmission power. Furthermore, we extend our research to adopt a digital sig- nature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

IV. SCHEME DESCRIPTION

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). Fig.6 presents a flowchart describing the EAACK scheme. All the nodes in the network are bidirectional. 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.

A. ACK

In Fig. 7, in ACK mode, node S first sends out an ACK data packet Pad1 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 Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, 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. *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. 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. As shown in Fig. 8, in S-ACK mode, the three consecutive nodes (i.e., A, B, and C) work in a group to detect misbehaving nodes in the network. Node A first sends out S-ACK data packet Psad1to node B. Then, snode B forwards this

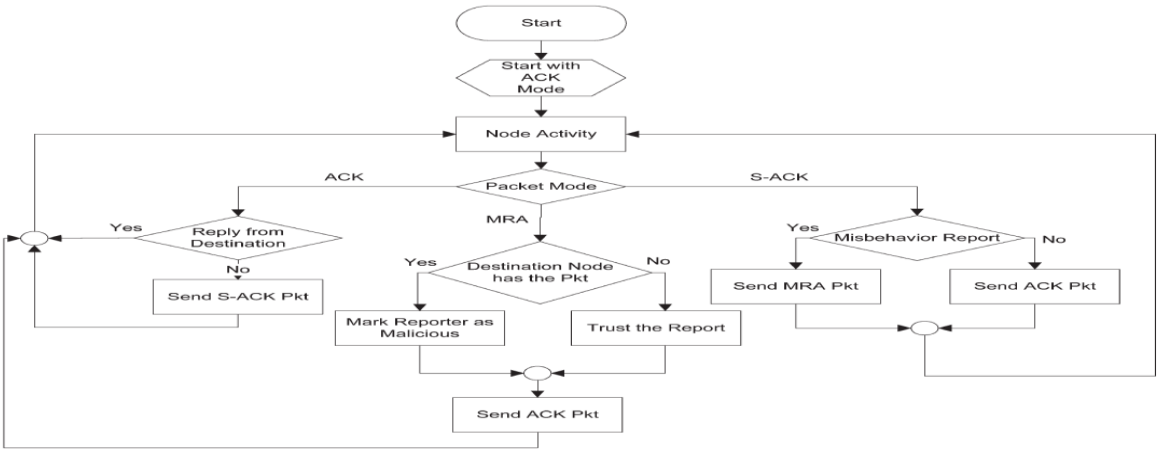

Fig 6: System control flow: this figure shows the system flow of how the EAACK scheme works.

packet to node C. When node C receives Psad1, as it is the third node in this three-node group, node C is required to send back an S-ACK acknowledgment packet Psak1 to node B. Node B forwards Psak1 back to node A. If node A does not receive this acknowledgment packet within a predefined time period, both nodes B and C are reported as malicious. EAACK requires the source node to switch to MRA 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 misbehavior report 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. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of

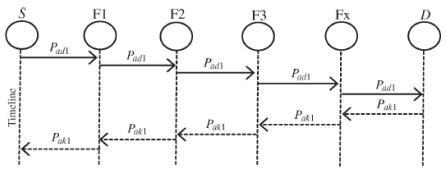

Fig7: ACK scheme: The destination node is required to send back an acknowledgement packet to the source node when it receives a new packet.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

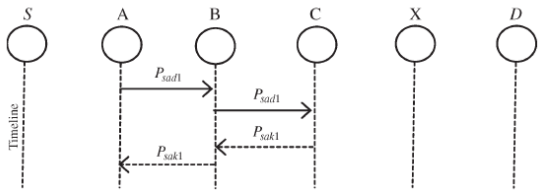

Fig 8: S-ACK node C required sending back an acknowledgement packet to node A.

detecting malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and un-tainted. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA [8] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

V. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially de- signed for MANETs. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme by using both DSA and RSA schemes.

REFERENCES

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

[2] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand rout- ing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[3] 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.

[4] 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.

[5] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[6] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbe- haviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–1s26, Feb. 1983.