International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Secured-Adaptive ACK Based Intrusion Detection System For MANETs Using Digital Signatures And MRA Concept

Savita P Jawale {savitapjawale@gmail.com}[1], Mrs. Rukmini Durgale {rukmini1dinu@gmail.com}[2]
[1] IV Sem, M.Tech, DCN, 2 Assistant Professor And Department of ECE, BTLIT, Bangalore-100.

ABSTRACT: The journey from wired network to wireless network has been a recent trend and necessity in the past few decades. The flexibility and scalability brought by wireless network made it possible in many applications. With the existing all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and exclusive applications. On the contrary to traditional network architecture, MANET does not require an immovable/static network infrastructure, each and every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. The nodes depend on their neighbors to transmit messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or any other emergency. However, the open medium and wide distribution of nodes make MANET susceptible to nasty attackers. 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, we strongly believe that it is vital to address its potential security issues. In this paper, it has been proposed and implemented a new intrusion-detection system named Secured Adaptive Acknowledgment (SAACK) specially designed for MANETs. Compared to present approaches, SAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances.

I. INTRODUCTION

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. Industrial remote access and control via wireless networks are becoming more and more popular these days .One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. But this communication is limited to the range of transmitters. This means that 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.

Fig 1.1 Wirelesses MANET

However, considering the fact that MANET is popular among critical mission applications, network security is of fundamental importance. regrettably, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. Let us take an example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is essential to develop an intrusion-detection system (IDS).

II. BACKGROUND

IDS in MANETs:

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to transmit 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, an 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

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

second layer in MANETs, and they are a great complement to existing proactive approaches.

TWOACK: TWOACK is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each 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 acknowledgement 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).

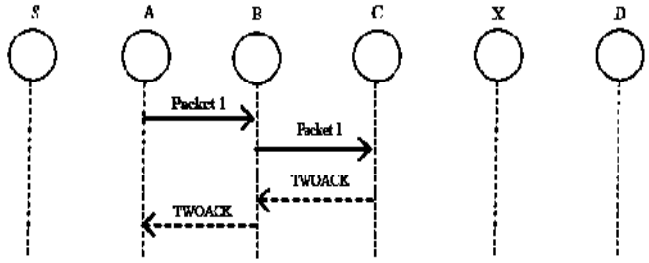

Fig 2.1 TWOACK

The working process of TWOACK is demonstrated in Fig 2.1.

AACK: It is based on TWOACK Acknowledgement (AACK) similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

III. EXISTING SYSTEM

Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Path rater. Watchdog acts as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously 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. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field.

DISADVANTAGES:

- Ambiguous collisions.
- Receiver collisions.
- Limited transmission power.
- false misbehavior report;
- collusion;
- Partial dropping.

IV. PROBLEM DEFINATION

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.

V. SCHEME DESCRIPTION

This section, describes the proposed SAACK scheme in detail. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. SAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in SAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 P, 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.

A. S-ACK: S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al. [15]. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement 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 demonstrated in Fig. 4.1, 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 to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehavior report, SAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

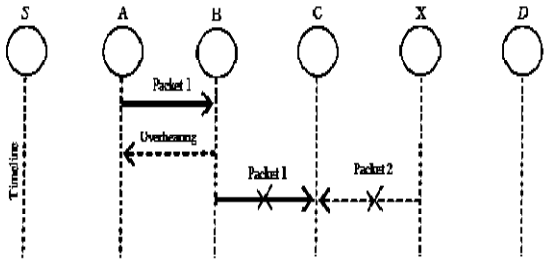

Fig. 4.1 Receiver Collisions: both node B and node X are trying to send packet 2 to node C at the same time

B. MRA : The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that 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. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other 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. By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. 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. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, SAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

C. Digital Signature : SAACK is an acknowledgement based IDS. All three parts of SAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviors in the network. Thus, it is extremely important to ensure all acknowledgement packets in SAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, [1] incorporated digital signature in their proposed scheme. In order to ensure the integrity of the IDS, SAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.

VI. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. In this paper, proposed a novel IDS named SAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. 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 . In order to seek the optimal DSAs in MANETs, we implemented both DSA schemes in proposed system . Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs

REFERENCES

[1]. 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.

[2]. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," 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 hoc networks: 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]. L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6]. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7]. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8]. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

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

[10]. 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.