

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.969 – 975

RESEARCH ARTICLE

EAACK—A Secure Intrusion-Detection System for MANETs

Mohammad Mubasheer¹, Solasu Sharavani²

¹ M.Tech 2nd Year, Dept. of CSE, TITS, JNTU, HYDERABAD, INDIA

² Assistant Professor, Dept. of CSE, TITS, JNTU, HYDERABAD, INDIA

¹ mubasheer.arsh143@gmail.com; ² shravanisolasu@gmail.com

Abstract— The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETWORK (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; 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. Otherwise, they rely on their neighbours to relay messages. The self configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious 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, 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 behaviour detection rates in certain circumstances while does not greatly affect the network performances. Mobile Ad hoc NETWORK (MANET).

Keywords— Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (EAACK) (EAACK), Mobile Ad hoc NETWORK (MANET)

I. INTRODUCTION

DUE TO THEIR natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. By definition, 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 [35]. One of the major

advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, 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.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14], [28]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. 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. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. 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 crucial to develop an intrusion-detection system (IDS)

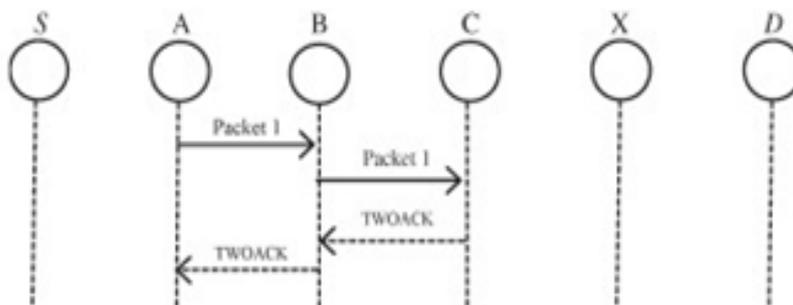


Fig 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

II. BACK GROUND

1. IDS in MANETs

As discussed before, 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, 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 second layer in MANETs, and they are a great complement to existing proactive approaches [27]. Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) [25].

1) Watchdog: Marti et al. [17] proposed a scheme named 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 Pathrater. Watchdog serves as an 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. When- ever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. [16] is one of the most important approaches among them network throughput.

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 receive collision. In this section, we discuss these three weaknesses in detail.

3) AACK: Based on TWOACK, Sheltami et al. [25] proposed a new scheme called AACK. 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 same network.

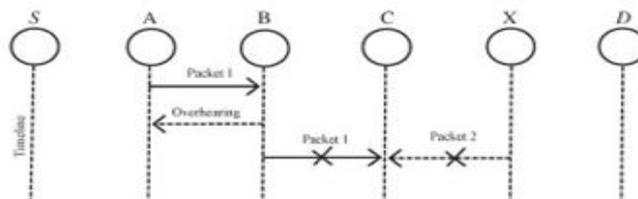


Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

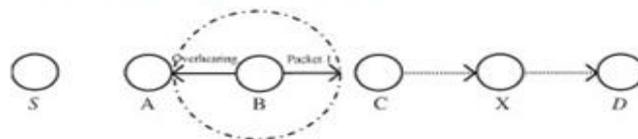


Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

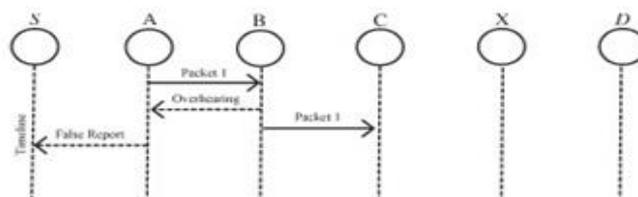


Fig. 6. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

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. 6. 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. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose a new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, we extend our research to adopt a digital signature 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

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work [12], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK.

According to the Internet draft of DSR [11], 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. Details are listed in Table I. Fig. 7 (shown later) presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is 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.

TABLE I
PACKET TYPE INDICATORS

| Packet Type | Packet Flag |
|--------------|-------------|
| General Data | 00 |
| ACK | 01 |
| S-ACK | 10 |
| MRA | 11 |

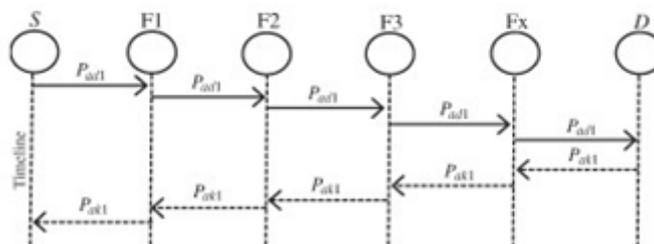


Fig. 7. System control flow: This figure shows the system flow of how the EAACK scheme works.

V. PERFORMANCE EVALUATION

During the simulation, the source node broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

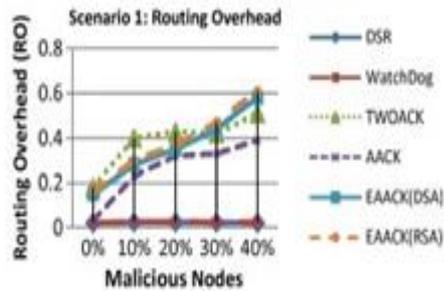


Fig. 11. Simulation results for scenario 1—RO.

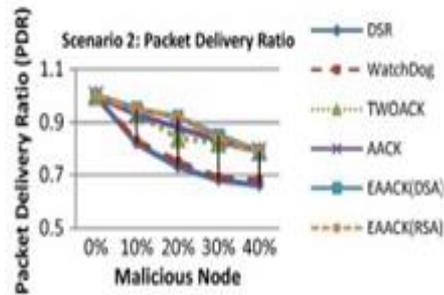


Fig. 12. Simulation results for scenario 2—PDR.

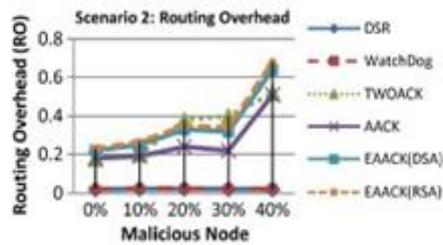


Fig. 13. Simulation results for scenario 2—RO.

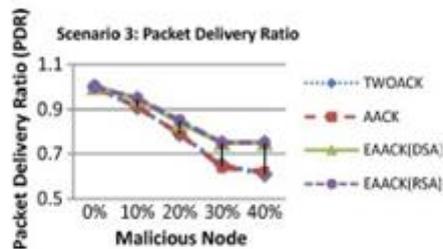


Fig. 14. Simulation results for scenario 3—PDR.

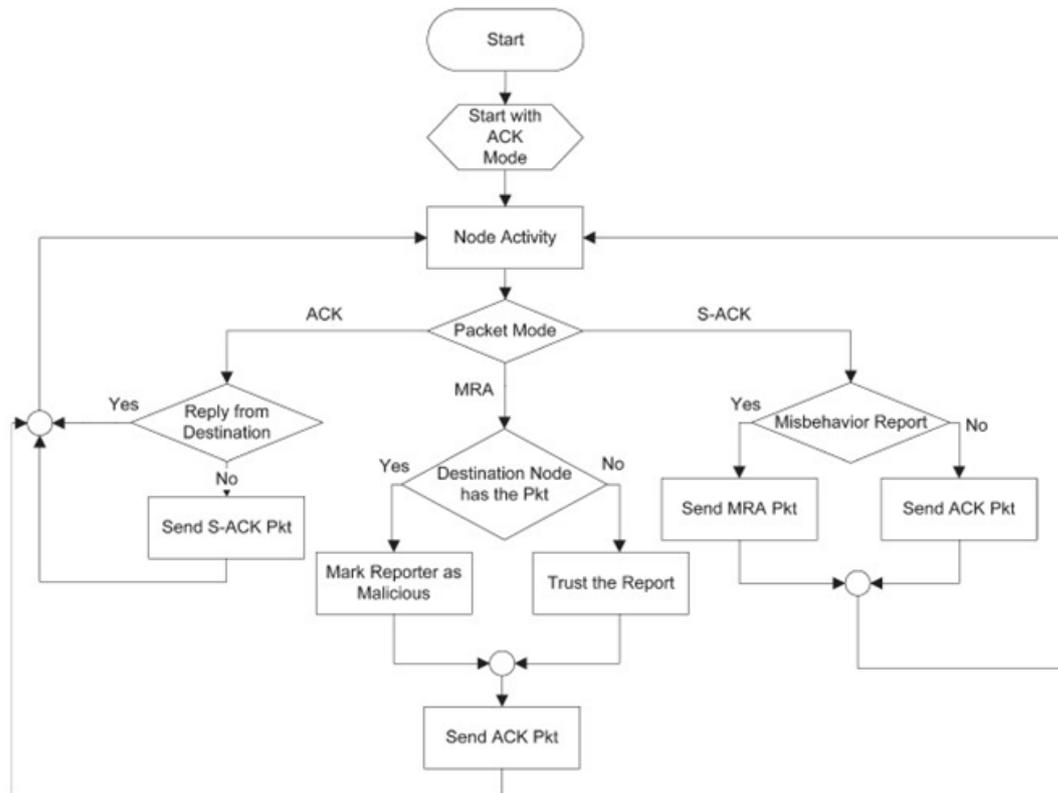


Fig 9. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

VI. C ONCLUSION AND FUTURE WORK

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 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. 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. Al-though 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. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs 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 our research work, we plan to investigate the following issues in our future research:

- 1) Possibilities of adopting hybrid cryptography techniques to further reduce the network verhead caused by digital signature;
- 2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys;
- 3) Testing the performance of EAACK in real network envi-ronment instead of software simulation.

REFERENCES

1. 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.
2. 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.
3. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.
4. L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
5. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Model- ing 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.
6. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:Challenges, design principles, and technical approach,"*Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.