A Survey on - A Secure Intrusion Detection Systems in Wireless MANETs

Nischitha A. R
M.Tech 4th Sem
Computer science and Engineering
Dr. AIT, Bangalore
Nischitha.ar@gmail.com

Harish Kumar H. C
Asst. Professor, Dept. of CSE
Dr. AIT, Bangalore
harishkumar.hc@dr-ait.org

***Abstract*-The migration to wireless network from wired network has been a global trend in the past few decades. Security has become an important part in Mobile Adhoc Networks because of their dynamic mobility, scalability and shared resources. MANETs is a collection of mobile nodes and it does not require a fixed infrastructure. So it acts as a dynamic topology for many applications. MANETs are highly vulnerable for attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Both Watchdog and TWOACK methods are not sufficient for protect MANETs in the cases of receiver collision, limited transmission power and false misbehavior report. To overcome such attacks the proposed technique is a secure intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed.**

Keywords—.AACK, EAACK, MANET, IDS, Receiver Collision, Watch Dog

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. MANET structure may vary depending on its application from a small, static network that is highly power constrained to a large-scale, mobile, highly dynamic network. Every node works 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 neighbors to relay messages. 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. 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 nodes to rely data transmission. There are two types of MANETs: closed and open.In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. Some resources are consumed quickly as the nodes participate in the functions.

MANET has two types of network, namely single-hop and multi-hop [1]. In a single-hop network, all nodes within the same radio range communicate directly with each other. In a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. A mobile ad-hoc network is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like military conflicts, emergency medical situations. However, the open medium of MANET is 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. Attackers can easily insert the malicious or incorporate nodes into the network to achieve attacks. Such misbehaving nodes need to be detected so that these nodes can be avoided by well behaved nodes. Many schemes and intrusion detection systems proposed to detect such nodes.

II. BACKGROUND

A. Intrusion Detection System

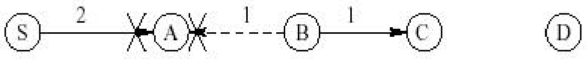
As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised 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. Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs.In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK , and Adaptive ACKnowledgment (AACK) .

1) Watchdog: In [5], Marti et al. proposed a reputation-based scheme. Two modules called watchdog and pathrater are implemented at each node, to detect and mitigate, respectively, routing misbehaviors in MANETs. Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet or not. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is.

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:

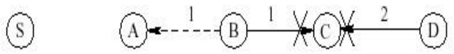
Ambiguous Collisions:

A packet collision occurs at the monitoring node

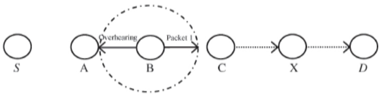


Receiver Collisions:

A packet collision occurs at the receiver. Both nodes B and D are trying to send packet 1 and packet 2, respectively, to node C at the same time.



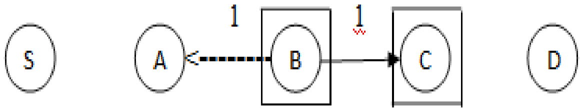
Limited Transmission Power:



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

False Misbehavior Report:

The Node A sends back a misbehavior report even though node B forwarded the packet to node C.



Partial Dropping:

Node keeps its tally just below the threshold and never is labeled as misbehaving

2) TWOACK :The TWOACK scheme can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

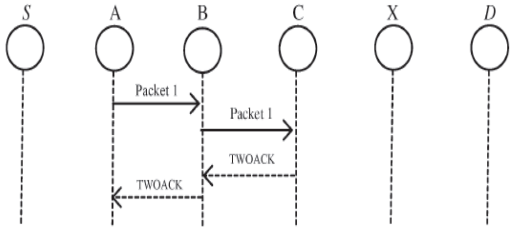


Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The 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 obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

3) AACK: Based on TWOACK, Sheltami *et al*, 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 throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2. In the ACK scheme shown in Fig. 2, the source node S sends out Packet 1 without any overhead except 2 b 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 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. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the 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).

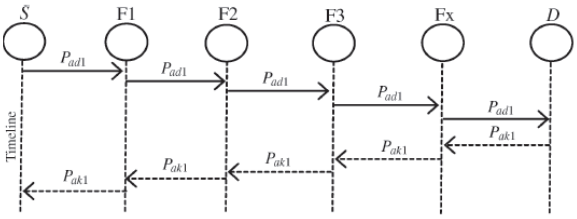


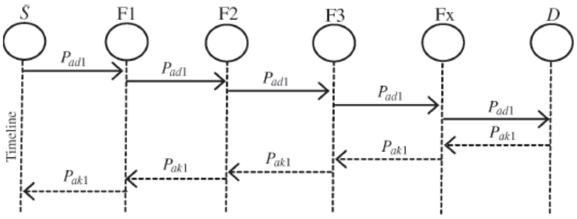
Fig.2. AACK

III.PROPOSED SYSTEM

The proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely receiver collision, limited transmission power and false misbehavior. In this section, we discuss these three weaknesses in details. In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in details. The approach described in this research paper is based on our previous work [8], where the backbone of EAACK was proposed and evaluated. EAACK is consisted of three major parts, namely ACK, S-ACK and Misbehavior Report Authentication (MRA).

A. ACK

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 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:

S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al. [8]. 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. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

C. 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. 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.

CONCLUSION

Malicious 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 designed 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.

REFERENCES

[1] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003. |

[2] O. Kachirski and R. Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p.57.1, January 2003. |

[3] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004. |

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp.255–265. |

[5] 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. |

[6] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, “On intrusion detection and response for mobile ad hoc networks,” in Proc. IEEE Int. Conf. Perform., Comput., 2004, pp. 747–752. |

[7] N. Kang, E. Shakshuki andT. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web-based Applications & Services (WAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2010. |

[8] Jin- Shyan Lee, "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008. |