IJDCST @ Dec, Issue- V-3, I-1, SW-01
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Adaptive Acknowledgment based Intrusion Detection System for MANETs

Syed Shajahan[1], Shaik Gousejohn [2]

[1] M.Tech(CSE), Nimra College of Engineering and Technology, A.P., India.

[2]Asst. Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering and Technology, A.P., India.

Abstract— Mobile Ad Hoc Network(MANET) is a kind of wireless network where you can find number of base stations which supports the communication of mobile nodes.. Several multi-hop routing protocols have been proposed for ad hoc networks, and most popular ones include: Dynamic Source Routing (DSR), Optimized Link-State Routing (OLSR), Ad Hoc On-Demand Distance Vector (AODV) and Destination- Sequenced Distance-Vector (DSDV). Most of these protocols rely on the assumption of a trustworthy cooperation among all participating nodes; unfortunately, this may not be a realistic assumption in real hosts. Malicious hosts could exploit the weakness of MANET to launch various kinds of attacks. Node mobility on ad hoc network cannot be restricted. As results, many Intrusion Detection System(IDS) solutions have been proposed for the wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. Thus, the wired network IDS characteristics must be modified prior to be implemented in the ad hoc network. Thus 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 vulnerabilities caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs. This paper presents an novel IDS for MANETs which is based on acknowledgements.

***Keywords*— ACK, Collision, Digital signature, IDS, MANET.**

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) is collection of wireless mobile nodes that are free to move in any directions at any speed. Mobile hosts are equipped with the wireless transmitter and a receiver that communicate directly with each other or forward message through other nodes. One of the major advantages of the mobile networks is to allow different nodes for data communications and still maintain their mobility. However, this communication is limited to the range of different transmitters. It means that two hosts cannot communicate with each other when the distance between the two hosts is beyond the communication range of their own. MANET solves this problem by allowing intermediate hosts to relay data transmissions. This is achieved by dividing MANET into two types of networks such as single-hop and multihop[1]. In a single-hop network, all the nodes within the same radio range communicate directly with each other. But in a multihop network, the nodes rely on other intermediate nodes to transmit if the end point node is out of their radio communication range [2].

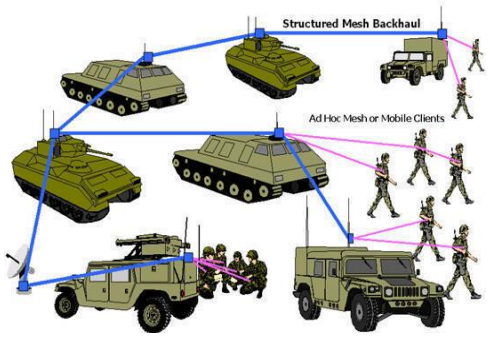

Figure 1: An example Mobile Ad Hoc Network

MANET is capable of operating a self-maintaining and self-organizing network without the need of any fixed infrastructure. Ad hoc networks does not require expensive base stations of infrastructure dependent network (single-hop wireless networks)[3]. As MANETs have different characteristics from the wired networks and even from single-hop wireless networks, there are more number of new challenges interrelated to security issues that need to be addressed. Initially, MANET was initially designed for military applications, but, in recent years, has found new usage. For example,

search and rescue mission, data collection, virtual classes and conferences where computers, laptops, PDA or other mobile devices are in wireless communication. Since ad hoc network is being used wide spread, security has become a very important issue. In general, MANETs are vulnerable based on the basic characteristics such as changing topology, open medium, absence of infrastructure, restricted power supply, and scalability. In such case, Intrusion detection can be defined as the process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is known an Intrusion Detection System (IDS) [4].

II. RELATED WORK

In [5], the authors suggested dynamic source routing protocol for the mobile adhoc networks. Because in the MANETs the mobile hosts are randomly moved. Due to the limited range of transmission one mobile host needs other mobile node to forward the data packets. The dynamic source routing protocol adjusts quickly to routing changes when node movement is frequent. But it requires little overhead during the frequent node movement. In [1], the authors proposed an Acknowledgment-based Approach to detect the routing misbehavior of the mobile adhoc networks. TWOACK is necessary to work on the routing protocols such as Dynamic Source Routing (DSR). The main idea of the two ACK method is when a node forwards a data packet, effectively through the next hop, the next-hop link of the destination node will send back a special two- hop ACK called 2ACK to specify that the data packet has been received successfully. In [6], the authors proposed a command filtering framework to allow or reject the human-issued commands so that unwanted executions are never performed. In this concept instead of using the client- server model the peer-to-peer (P2P) communication between mobile robots is used.

In [7], the authors proposed Collaborative Security Architecture for detecting the Black hole attack in the mobile adhoc networks. In this technique, if the node forwards the data packet to the watchdog node identifies whether the next node also forwards the data packet. If the next node does not forwards that data packet the watchdog node makes it is as the misbehavior node. In [8], the authors proposed Intrusion detection system for the MANETs. In the absence of the fixed infrastructure to provide communications, MANET is an attractive technology for some applications like environmental monitoring, conferencing, military applications. In [9], the authors suggested a model to detect the node misbehavior in the mobile adhoc networks. Based on the Sequential Probability Ratio Test, the authors develop a model to describe how nodes can differentiate between the routes that include misbehaving nodes and routes that do not. For the detection of the misbehaving hosts in the infected routes a centralized and a localized approach is used. In [10], the authors suggested secure routing and the intrusion detection system in the adhoc networks. The authors present a proof-of-concept implementation of a secure routing protocol based on AODV over IPv6 for the Intrusion Detection and Response system for ad-hoc networks.

PROPOSED WORK

A. Problem Definition

Our proposed method is designed to tackle false misbehavior and receiver collision.

Receiver Collisions

Node A sends Packet 1 to node B, it tries to overhear if node B forwarded that packet to another node C; meanwhile, node X is forwarding Packet 2 to the node C. In such case, node A overhears that the node B has successfully forwarded Packet 1 to node C but failed to detect that the node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C. This is shown in figure 2.

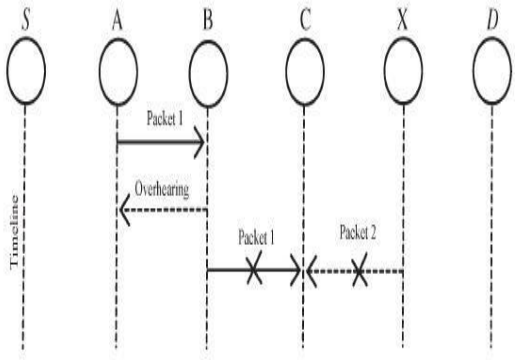

Figure 2: Receiver Collision

False Misbehavior Report

Node A successfully overheard that the node B forwarded Packet 1 to node C, node A still reported node B as misbehaving. Due to the open medium

and remote distribution of typical MANETs, the attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. This is shown in figure 3.

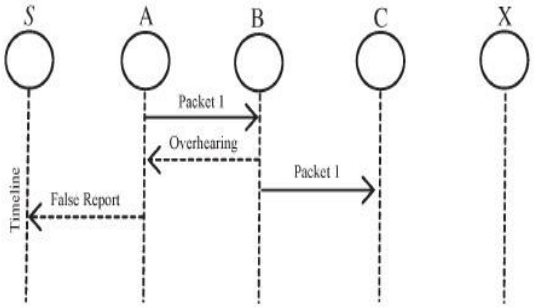

Figure 3: False Misbehavior Report

Our proposed work is consisted of three major components, namely, ACK, secure ACK, and misbehavior report authentication(MRA).

B. ACK

ACK is essentially associate end-to end acknowledgment scheme used in our work. It acts as a district of the hybrid scheme in this work, attending to scale back network overhead once no network misconduct is detected. In Figure 4, in ACK mode, node S initial sends out associate ACK information packet Pad1 to the destination node D. If all the intermediate nodes on the route between the nodes S and D square measure cooperative and node D with success receives Pad1, the node D is needed to remand associate ACK acknowledgment packet Pak1 on a similar route however in a very reverse order. Inside a predefined fundamental quantity, if the node S receives Pak1, then the packet transmission from node S to the node D is winning. Otherwise, node S can switch to S-ACK mode by causing out an associate S-ACK information packet to sight the misbehaving nodes within the network route.

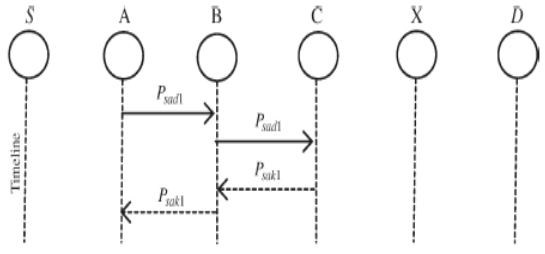

Figure 4: ACK scheme

C. S- ACK

S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect the misbehaving nodes. For each three consecutive nodes in the network route, the third node is required to send the S-ACK acknowledgement packet to the first node .The intention of introducing the S- ACK mode is to detect misbehaving nodes in the presence of receiver collision.

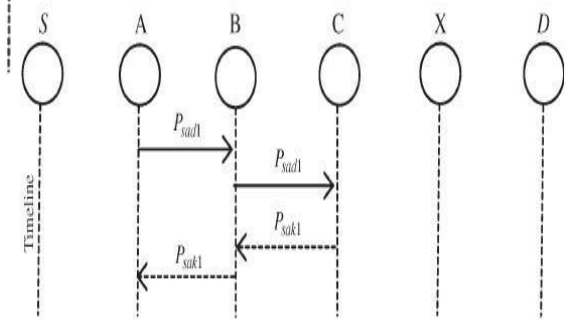

Figure 5: Secure ACKnowledgement

D. MRA

Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, our work requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect such false misbehavior. The MRA field is designed to resolve the weakness of the Watchdog when it fails to detect misbehaving nodes with the presence of the false misbehavior. The false misbehavior report can be generated by the malicious attackers to falsely report innocent nodes as malicious. The core of the MRA field is to authenticate whether the destination node has received the reported missing packet through a different network route. To initiate the MRA mode, the source node first searches its local knowledge base and then seeks for an alternative route to the destination host. If there is no other that exists, then the source node starts a DSR routing request to find another route.

E. Digital Signature

Our proposed work is an acknowledgment-based IDS. They all rely on the acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all ACK packets are authentic and untainted. In order to ensure the integrity of the detection system, our work requires

all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

III. CONCLUSION

MANET is a collection of wireless mobile nodes forming a network without the need of existing infrastructure. There are various challenges that are faced in the MANET environment. These are mostly due to the lack of the resources of these networks. They are usually set up in situations of emergency, for temporary operations or in a case if there are no resources to set up elaborate networks. The solutions for traditional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of network communication and lack of any security infrastructure raise several security problems. This paper focuses on the acknowledgment based IDS for MANETs. The proposed method provides higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

REFERENCES

[1] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[2] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE

[3] 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.

[4] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[5] 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.

[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] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.

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

[9] 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

[10] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Commun, 2005, pp. 191–199.