An Effective Trust Based Intrusion Detection System for Mobile Adhoc Network

D.Ayyamuthukumar M, E.,(Ph.d)
Associate Professor
Department of Computer Science
KSR College of Technology
Tirucengode.

K.GirijaB.Tech.,(M.E)
Department of CSE
KSR College of Technology
Tirucengode
girijasivakumar2013@gmail.com

Abstract

A mobile adhoc network is an autonomous network that consists of nodes which communicate with each other with wireless channel. Due to its dynamic nature and mobility of nodes, mobile adhoc networks are more vulnerable to security attack than conventional wired and wireless networks. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors 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. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose t 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.

I. INTRODUCTION

A Mobile Ad hoc Network, or MANET, consists of agroup of cooperating wireless mobile hosts (nodes) thatdynamically constructs a short lived and self-configuringnetwork without the support of a centralized networkinfrastructure. The mobile nodes can be cell-phones, PDAsand laptops and typically support several forms of wirelessconnectivity like 802.11, IrDA, Bluetooth, etc.

One advantage of wireless networks is the ability totransmit data among users in a common area whileremaining mobile. However, the range of transmitters ortheir proximity to the wireless central points limits thedistance between peers. Mobile Ad hoc networks mitigatethis problem by allowing out of range nodes to route datathrough intermediate nodes, i.e., each send its own data aswell as routes and forwards data on behalf of other nodes.

The MANET may operate in a standalone fashion, ormay be connected to the larger Internet. Minimalconfiguration and quick deployment make ad hoc networkssuitable for using in emergency circumstances where aninfrastructure is unavailable or unfeasible to be installed likenatural or human-induced disasters, military conflicts and medical emergency situations. There have been significant improvements related to the different characteristics and topics in MANET, particularly in the fields related to routing protocols, clustering protocols, location and mobility prediction. However, the security aspects of MANET have been rarely addressed. The security goals of MANET include availability, integrity, authentication, confidentiality and non-repudiation.

One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design.These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. This last point is where the main problem for MANET security resides: the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry .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 thatmost routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or noncooperative 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) specially designed for MANETs.

II. BACKGROUND

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 he 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. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgment (AACK).

1)Watchdog:

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. Whenever 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. The Watchdogscheme 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.

2)TWOACK:

TWOACK is neither an enhancement nor aWatchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links byacknowledging 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. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). 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.

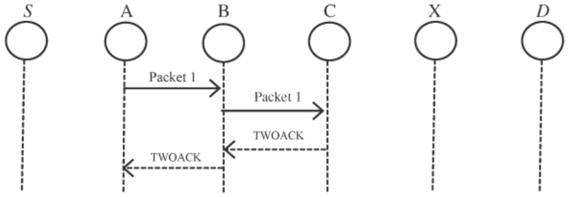

Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

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:

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 schemein ACK is shown in Fig. 2.

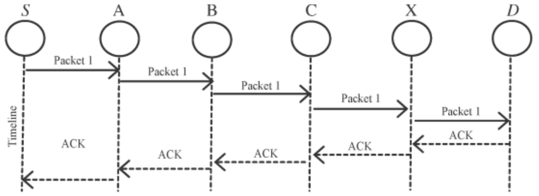

Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

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 thatthey 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).

B. Digital Signature:

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and nonrepudiation. Digital signature is a widely adopted approach to ensure theauthentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature.

Digital signature schemes can be mainly divided into the following two categories.

1) *Digital signature with appendix*: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).

2) *Digital signature with message recovery*: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA.

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 a typical example of receiver collisions, shown in Fig. 4, 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 butfailed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

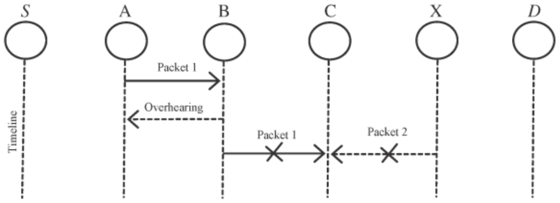

Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

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. 5.

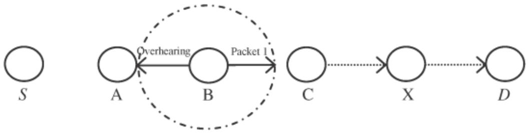

Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

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.

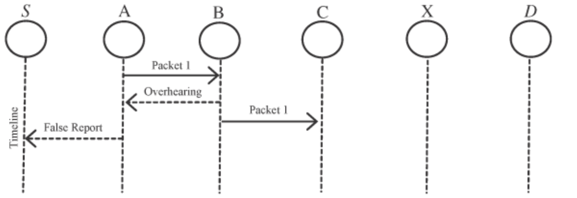

Fig. 6. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C

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 arevulnerable 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 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).

A. ACK

As discussed before, 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 Fig. 8, in ACK mode, node S first sends out an ACK data packet *Pad*1 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 *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, 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.

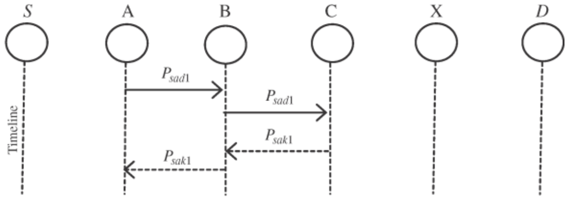

Fig. 8. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK. The principle is to let everythree 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 todetect 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. This is a vital 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 generated by malicious attackers to falsely reportinnocent 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 the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to thenature 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 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 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. They allrely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

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 digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

V.CONCLUSIONAND 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 designed for MANETs and compared it against other popular mechanisms. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limitedtransmission 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 and RSA schemes. 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 techniquesto further reduce the network overhead caused by digitalsignature;

2) examine the possibilities of adopting a key exchangemechanism to eliminate the requirement of predistributedkeys;

3) testing the performance of EAACK in real network environmentinstead of software simulation.

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] 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.

[3] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting forged acknowledgements in MANETs,” in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “Anacknowledgment-based approach for the detection of routing misbehavior in MANETs,” *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

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

[6] N. Nasser and Y. Chen, “Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network,” in *Proc. IEEE Int.Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[7] 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.,Commun.*, 2004, pp. 747–752.