International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)
Research Article | **May 2014**

An Assure Encroachment Sensing Scheme for MANET'S

K.Gayatri*, A.Madhava Reddy, V.Venkatalakshmi
MCA Department, JNTUK
India

Abstract—

Among all the contemporary wireless net- works, 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. 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.

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

I. INTRODUCTION

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 [10]. 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 par- ties 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. . MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [2]. 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. 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. Many research efforts have been devoted to such research topic [1],[4].

II. BACKGROUND

A. 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, 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. 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: Marti *et al.* [5] 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 IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours 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. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme.

Nevertheless, as pointed out by Marti *et al.* [5], the Watchdog scheme fails to detect malicious misbehaviours with the presence of the following: 1) ambiguous collisions; 2) receiver collisions;
3) Limited transmission power; 4) false misbehaviour report; 5) Collusion; and 6) partial dropping. We discuss these weaknesses with further detail in Section III.

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.* [4] is one of the most important approaches among them. On the contrary to many other schemes, 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 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) [3].

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.

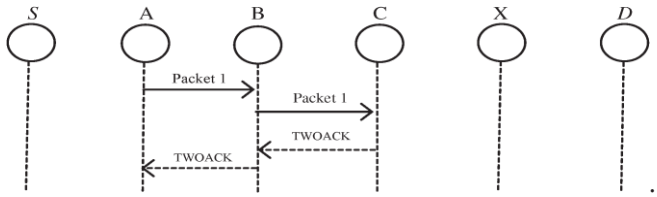

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it

3) AACK: Based on TWOACK, Sheltami *et al.* [8] pro- posed 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 fact many of the existing ids in MANETS adopt an acknowledgement 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).

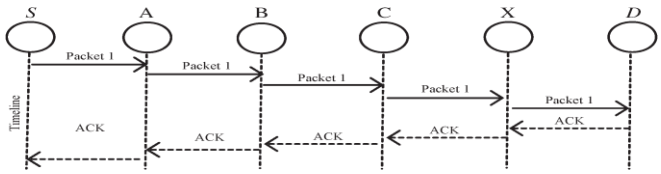

Fig.2 ACK scheme: The destination node is required to send acknowledgement packets to the source node

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 [6].
In this we implemented both DSA and RSA in our proposed EAACK scheme. The main purpose of this implementation is to compare their performances in MANETs. First, a fixed-length message digest is computed through a preagreed hash function *H for* every message *m*. This process can be described as

$$H(m) = d. \qquad (1)$$

Second, the sender Alice needs to apply its own private key $Pr-Alice$ on the computed message digest *d*. The result is a signature Sig_{Alice} , which is attached to message *m* and Alice's secret private key

$$S_{Pr-Alice}(d) = Sig\text{Alice} \qquad (2)$$

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $Pr-Alice$ as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.

Next, Alice can send a message *m* along with the signature Sig_{Alice} to Bob via an unsecured channel. Bob then

computes the received message m^t against the preagreed hash function H to get the message digest d^t. This process can be generalized as

$$H(m^t) = d^t. \quad (3)$$

Bob can verify the signature by applying Alice's public key $P_{k-Alice}$ on Sig_{Alice}, by using

$$S_{P_{k...Alice}}(Sig_{\text{Alice}}) = d. \quad (4)$$

If $d == d^t$, then it is safe to claim that the message m^t transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

III. PROBLEM DEFINITION

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehaviour, limited transmission power, and receiver collision.

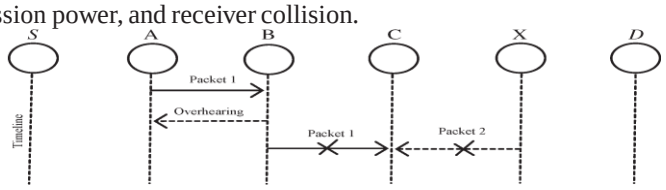

Fig 3. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

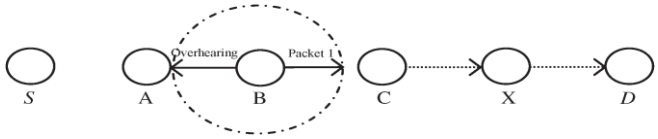

Fig.4. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

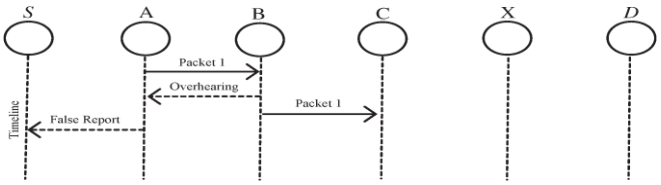

Fig.5. False misbehaviour report: Node A sends back a misbehaviour report even though node B forwarded the packet to node C.

In a typical example of receiver collisions, shown in Fig. 3, 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 but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

In the case of limited transmission power, in order to pre- serve 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. 4.

For false misbehaviour 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. 5. 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 misbehaviour report attack.

IV. SCHEME DESCRIPTION

In this section, we describe our proposed EAACK scheme in detail. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK.

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 misbehaviour is detected. In Fig. 8, in ACK mode, node S first sends out an ACK data packet P_{ad1} 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 P_{ad1}, node D is required to send back an ACK acknowledgment packet P_{ak1} along the same route but in a reverse order. Within a predefined time period, if

node S receives P_{ak1} , 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.

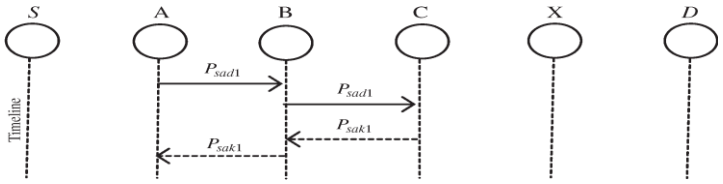

Fig. 6. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

B. S-ACK (Secure Acknowledgement)

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [4]. The principle is to let every three 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 to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA (Misbehaviour Report Authentication).

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. By adopting an alternative route to the destination node, we circumvent the misbehaviour 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 misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted.

D. Digital Signature

All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviours 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. . 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 [9] and RSA [7] digital signature schemes in our proposed approach.

VI. CONCLUSION 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 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.

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 overhead caused by digital signature;
2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys;
3) Testing the performance of EAACK in real network environment instead of software simulation.

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.

[2] 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.

[3] 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.

[4] 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.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Ann. Int. Conf. Mobile ComputNetw.*, Boston, MA, 2000, pp. 255–265.
[6] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.
[8] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
[9] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal In- formation Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
[10] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. In strum. Meas.*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008