An Acknowledgment Based Secure Intrusion Detection System for MANETs

T. Sathiyabala[#1], A. Lourdes Mary[#2]
[1]PG Scholar,
[2]Associate Professor,
[#]Department of Computer Science and Engineering, Anna University-Chennai,
SCAD College of Engineering and Technology,
Cheranmahadevi, Tamilnadu, India.

Abstract **- In recent years mobile ad hoc networks (MANETs) have become a very popular research topic. It provides communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to other approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances. The project proposes a hybrid encryption technique to reduce the network overhead caused by digital signature in EAACK.**

Key Words: RSA Advanced Encryption Standard, AODV, MANETs, Asymmetric Encryption, Misbehavior Report Authentication (MRA).

I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS is software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic that violates acceptable use policies [1]. Many IDS tools developed will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN)[3].

In such a network, a set of mobile nodes are connected to a fixed wired structure. WLANs have a diminutive range and are usually deployed in places such colleges, offices, cafeterias, etc. One among the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility [4]. On the other hand, this communication is limited to the range of transmitters and receivers. This means that nodes cannot communicate with each other when the distance between the nodes is beyond the communication range of their network. MANET solves this problem by allowing intermediate parties to relay data transmissions. MANET is partitioned into two types of networks, namely, single-hop, multihop networks. Single-hop network allows all nodes within the same radio range communicate directly with each other. And in the multihop network, nodes transmitted to other intermediate nodes if the destination node is out of their transmitting range.IDSs usually act as the second layer in MANETs, and it is a great accompaniment to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs

Due to the nodes lack of substantial protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Particularly, 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. If MANET can detect the attackers as soon as they enter the network, it will be able to wholly eliminate the potential damages caused by compromised nodes at the first time. IDSs typically act as the second layer in MANETs, and they are a great balance to existing proactive approaches [7]. The proposed design focuses on reducing the network overhead caused by the digital signature [20].

The public key cryptographic algorithm is used here. The public key cryptographic algorithms are more secure than symmetric algorithms. Because, it has two keys one for encryption and another one for decryption [19]. In this hybrid encryption technique we propose symmetric encryption for encryption/decryption and using public key cryptosystems for authentication.. The IDS (Intrusion Detection System) suitable for networks, which detect nodes Misbehavior, anomaly in packet forwarding such as intermediary nodes dropping or delaying packets approaches. The public key encryption is used in the secure transmission. The proposed key encryption focuses on reducing the network overhead caused by the digital signature.

II. RELATED WORK

In the related work, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

WATCHDOG

The projected scheme named Watchdog that aims to advance throughput of network with the presence of malicious

nodes. The watchdog scheme is categorized into two parts, such as Watchdog and Pathrater. Watchdog performs as an intrusion detection system for MANETs [18]. It is in charge for detecting malicious nodes misbehaviors in the network. The Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. Certainly Watchdog node overhear that its next node fails to for-ward the packet within a certain period of time, it in-creases its failure counter. Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are besides based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of

- False misbehavior report
- Limited transmission power
- Receiver collisions
- Ambiguous collisions
- Collusion,
- Partial dropping

TWOACK

TWOACK is neither an enhancement nor a Watch-dog base scheme. It aims to resolve the limited transmission power and receiver collision problems in Watchdog; TWOACK detect the misbehaved links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination [1]. On the retrieval of a packet, each node all along the route is required to send back an acknowledgement packet to then ode that is two hops away from it down the route. TWOACK is necessary to work on routing protocols such as Dynamic Source Routing (DSR)

AACK

It is based on TWOACK Acknowledgement (AACK) alike to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end to end acknowledgement scheme called ACK. AACK, significantly reduced network overhead compared to TWOACK, still it is capable of maintaining or even surpassing the same network throughput. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still bear from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets [5].

III. PROBLEM DEFINITION

This approach is tackled three of the six weaknesses of Watchdog scheme, such as false misbehavior, receiver collision and limited Transmission power. In this section, we confer these three weaknesses in details. In a typical example of receiver collisions, demonstrated in Fig. 1, after node A sends Packet1 to node B, it tries to overhear if node B forwarded this packet to it tries to node C; in the meantime, node X forward packet 2 to node C .In such case, node A overheads that node B has successfully, forwarded packet 1 to node C, failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

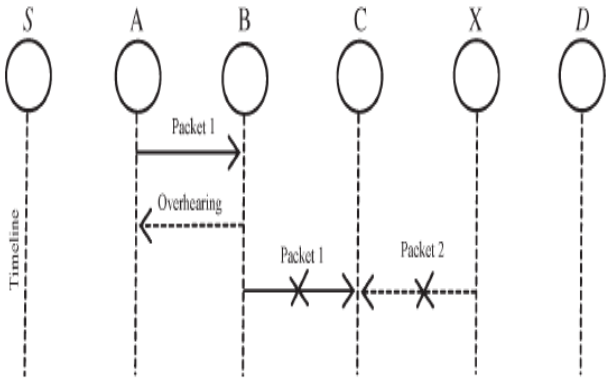

Fig 1: Receiver collisions: both node B and node X are trying to send packet 2 to node C at a time.

During the case of limited transmission power, in order to preserve its own battery resources, node B purposely limits its communication power so that it is strong enough to be overheard by node A but not strong enough to be received by node C. For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, the node A still report the node B as misbehaving as shown in Fig1. Due to the open standard and remote distribution of typical MANETs, attackers can easily confine and compromise one or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, AACK and TWOACK solve two of these three weaknesses, namely limited transmission power, receiver collision [2]. Though, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to s propose a new intrusion detection system specially considered for MANETs, which solves not only limited transmission power and receiver collision, but also the false misbehavior problem.

The acknowledgment packets are valid and authentic by using digital signature. In this research work, our goal is to propose a IDS specially designed for MANETs, which solves routing overhead caused by digital signature but also improve the security in system.

IV. PROPOSED SYSTEM

The proposed design focuses on reducing the network overhead caused by the digital signature. The public key cryptographic algorithm is used here. The public key cryptographic algorithms are more secure than symmetric algorithms [14]. Because, it has two keys one for encryption and another one for decryption. In this hybrid encryption technique we propose symmetric encryption for encryption/decryption and using public key cryptosystems for authentication. The ultimate goal of the security solutions for wireless networks is to provide security services, such as privacy, reliability, and authenticity [4].

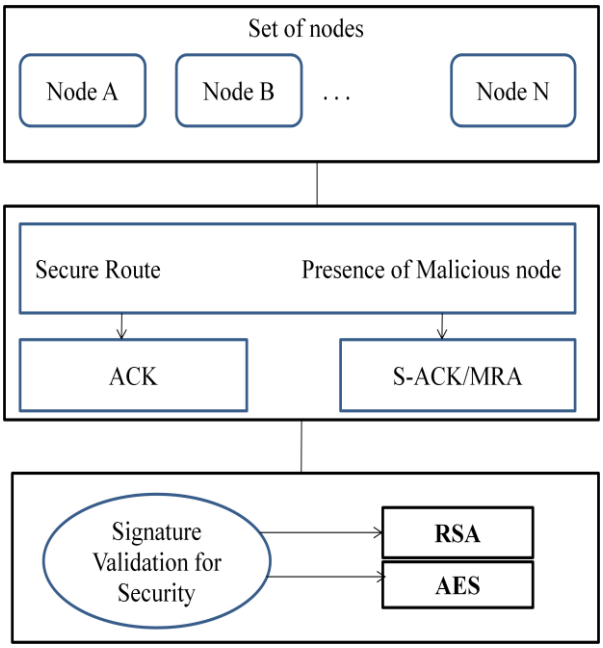

Fig 2. Architecture of EAACK.

EAACK consists of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA)

ACK IMPLEMENTATION

ACK is basically an end-to-end acknowledgment scheme [11] .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected. The basic flow is if source Node A sends a packet p1 to destination Node D, if the entire intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A), if ACK from the destination get delayed then it S-ACK process will be initialized.

S-ACK (Secure ACK)

S-ACK scheme is an enhanced version of TWOACK scheme .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 requisite to send an S-ACK acknowledgement packet to the first node. The use of introducing S-ACK mode is to detect misbehaving nodes in the occurrence of receiver collision or limited transmission power.

MISBEHAVIOR REPORT AUTHENTICATION (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. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious [1]. This attack can be fatal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA system is to authenticate whether the destination node has received the reported lost packet through a different path.

First the secure route for data transmission should be found. The source sends a data to the destination for route identification to the destination. Route identification based on AODV (Ad hoc On-demand Distance Vector routing protocol) protocol model [16]. AODV protocol (Ad hoc On Demand Vector) protocol is implemented for finding routes in the MANET [9]. The routing protocol is designed for use in mobile ad-hoc network of that even contains thousands of nodes. Route discovery mechanism [10] is invoked only if a route to destination is known. Each node maintains a routing table that contains information about reaching the destination nodes and this node act as both a host and a routing node. It's a reactive protocol.

AODV belongs to the class of Distance Vector Routing Protocol (DV).In a DV every node known its neighbors and the costs to reach them. The node maintains its own routing table, storing all nodes in the network, distance and the next hop to them. If the node is not reachable the distance to it is set to infinity. After getting a secure route, the data send securely to the destination by using hybrid encryption cryptographic techniques [8]. The data that send from the source node will be encrypted with RSA and AES techniques before its travelling to the destination node. The received data will be decrypted with RSA and AES in the destination node. After receiving the data at destination, the destination node required to send an acknowledgement packet to the source. In presence of malicious node, sender node cannot be defined the route. So that routing overhead is reduced in hybrid technique compared with DSA in EAACK [7].

V. PERFORMANCE EVALUATIONS

In this section, it is concentrated on describing our simulation environment and methodology as well as the comparing performances through simulation result comparison with Watchdog, TWOACK and EAACK schemes. In order better compare the simulation results with other research works, the default scenario settings in NS 2.34 is adopted. The aim is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration assigned of 50 nodes.

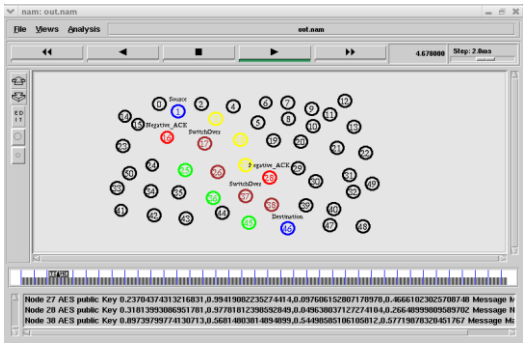

Fig 3. Optimized path without malicious nodes

By comparing with the other Intrusion Detection systems used, this proposed work enhances the performance by increasing the throughput. The Response time increases in the transmission by implementing the asymmetric encryption [11]

techniques to reduce the network of network overheads caused by the digital signature scheme and also by using the AODV protocol the optimized paths are used in transmission [17]. And the AODV protocol works better in the presence of higher mobility scenario. In order to measure and compare the performance of our proposed scheme, we adopt the following two performance metrics,

Packet Delivery Ratio (PDR): PDR defines the ratio of the number of packets the destination received and the number of packet sent by the source

Routing Overhead (RO): RO defines the ratio of the Amount of routing related transmissions (RREQ, RREP, RERR, ACK, S-ACK and MRA.

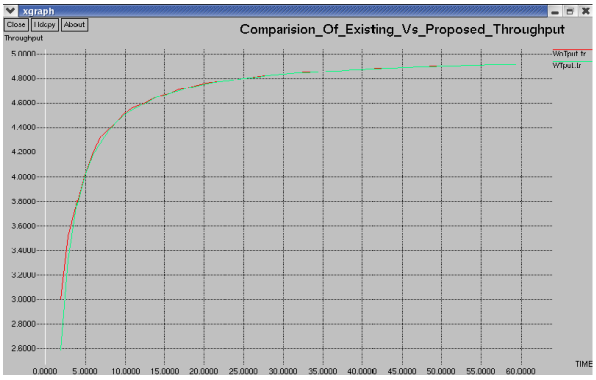

Fig 4. Increased throughput

VII. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. The proposed novel IDS named EAACK controls the network overhead that caused by digital signature. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of false misbehavior report. Limited Transmission power, Receiver collision. To prevent the attackers from initiating forged acknowledgment attacks, the hybrid cryptographic scheme is introduced in this scheme. It can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. In order to take optimal path AODV protocol is used to improve the performance of mobility in MANETs.

To increase the merits of the work, it is planned to investigate the following issues in our future research:

1) Inspect the possibilities of adopting a Key exchange mechanism to eliminate the requirement of pre distributed keys;
2) Testing the performance of EAACK in real network environment instead of software simulation

REFERENCES

[1] Elhadi M. Shakshuki, Senior Member,IEEE, Nan Kang, and Tarek R. Sheltami, IEEE; "EAACK—A Secure Intrusion-Detection System for MANETs";IEEE Transactions on industrial lectronics, VOL. 60, NO. 3, March 2013.

[2] 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, pp. 4266–4278, Oct. 2009.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer- Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, "Security and Cooperation in Wireless Networks." Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modelingand 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

[7] 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*

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vectorrouting for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.*

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routingprotocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom,*Atlanta, GA, 2002, pp. 12–23.

[10] 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.

[11] 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.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodesin MANETs, In *Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10*,2010, pp. 216–222.

[13] 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

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc communications*in AEC industry," *J. Inf. Technol. Const., vol. 9, pp. 313–323,*2004.

[15] 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.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-basedapproach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput., vol. 6, no. 5,* May 2007.

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

[18] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.Raton, FL: CRC, 1996, T-37.*