Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

EAACK-A Secure Intrusion-Detection System For MANETs

Vidhu K. Vikram[1], Jeslin P. Jo[2]
[1]*PG Student, Department of ECE, FISAT,Angamaly*
[2]*Asst. Professor, Department of ECE, FISAT*

Abstract— The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, 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. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. 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, it is strongly believed that it is vital to address its potential security issues. This paper proposes 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 (AACK) (EAACK), Mobile Ad hoc NETwork (MANET)

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) , by definition is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicates with each other through bidirectional wireless links either directly or indirectly. Industrial remote access and control through wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its capacity to allow data communication between different parties and still maintain their mobility. But the communication of wireless networks is limited to the range of transmitters. This means that two nodes cannot directly communicate when the distance between the two nodes is beyond the communication range of the two nodes. MANET overcomes this drawback by allowing intermediate parties to relay transmission of data. This is achieved by dividing MANET into two types of networks viz- single-hop and multihop. In the former network, all nodes within the same radio range communicate directly with each other. On the other hand, in the latter network, nodes rely on other intermediate nodes to transmit if the destination node is beyond their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a centralized infrastructure; thus, all nodes are free to move randomly.

Small amount of configuration and fast deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable to install in scenarios like natural or human-induced disasters, military conflicts, and hospital emergency situations. MANET is becoming more and more widely and quickly implemented in the industry because of its unique characteristics

and also considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Still, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the lack of nodes' physical protection, malicious attackers can easily capture and compromise communication of nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network works cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting attackers or noncooperative nodes into the network. Furthermore, because of MANET's distributed architecture and randomly changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In cases like this, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. RELATED WORK

Nodes in MANETs assume that other nodes relay data by always cooperating with each other because of the limitations of most MANET routing protocols,. This assumption leaves the attackers with the opportunities to give a significant impact on the network by compromising just one or two nodes. To overcome this problem, there should be an IDS to increase the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely detect malicious nodes thus eliminating the potential damages caused by compromised nodes at the first time. IDSs usually is the second layer in MANETs, and they are a great complement to existing proactive approaches [27].A very thorough survey on contemporary IDSs in MANETs was presented by Anantvalee and Wu [4]. This section mainly describes three existing IDS approaches. They are Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) [25].

1.1. Watchdog

This scheme is designed to improve the throughput of network with the presence of malicious nodes.The Watchdog scheme has two parts- Watchdog and Pathrater. Watchdog serves as an IDS for MANETs and is responsible for detecting malicious nodes in the network. Watchdog detects misbehaving nodes by listening to its next hop's transmission. If this node overhears that its next node doesn't forward the packet within a time period, its failure counter is increased and , the Watchdog node reports it as malicious, whenever a node's failure counter exceeds a predefined threshold. In such case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future data transmission. Furthermore, compared to some other intrusion detection schemes, Watchdog is capable of detecting misbehaving nodes rather than links. These abilities have made this IDS a popular choice in the network field and also it is seen that many MANET IDSs are either based on or a development to this scheme [15], [20], [21], [25]. Nevertheless, as pointed out by Marti et al. [17], this scheme fails to detect attacking nodes 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.

2.2. TWOACK

Many researchers proposed new methods to solve the above weaknesses of Watchdog scheme and one among them is the scheme named TWOACK proposed by Liu et al. [16].

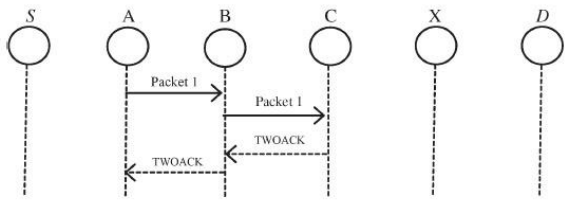

Figure.1. TWOACK Scheme

TWOACK is neither an enhancement of Watchdog nor a Watchdog-based scheme. TWOACK detects misbehaving links (not nodes) 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) [11]. 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. 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. However, many research studies are working in energy harvesting to deal with this problem [25], [28], [29].

2.3. AACK

Based on TWOACK, Sheltami et al. [25] 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 Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node. 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.

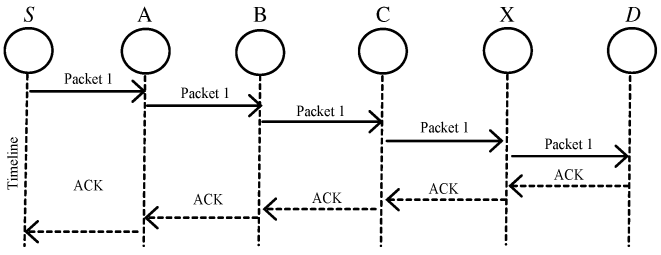

Figure.2.AACK Scheme

2.4. Digital Signature

Digital signatures have always been and also an integral part of cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [18]. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non repudiation 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 [33]. 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) [33].

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 [23].

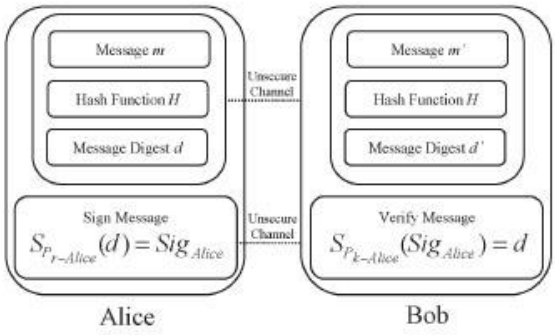

Figure.3.Communication With Digital Signature

For digital signature,both RSA and DSA schemes are used.DSA is an example oof digital signature with appendix i.e.,the original message is required in the signature verification algorithm. RSA is an example of digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. But digital signature incorporates slight overhead to the network-mainly RSA digital signature scheme. In this research work, we implemented both DSA and RSA in our proposed EAACK scheme. The main purpose of this implementation is to compare their performances in MANETs. The general flow of data communication with digital signature is shown in Fig. 3.

III. PRELIMINARY

This section defines the notations used in this paper.

3.1.Notations

The notations used in this paper are:

Table 1. Notations Used

Acronym	*Description*
MRA	Misbehavior Report Authentication
DSR	Dynamic Source Routing
RSA	Rivest-Shamir Adleman
DSA	Digital Signature Algorithm

IV. 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 this section, we discuss these three weaknesses in detail.

4.1.Receiver Collision

This problem is shown in figure 4 below. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

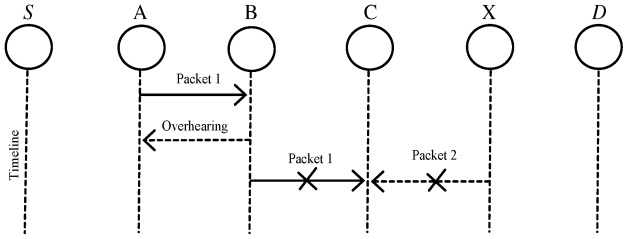

Figure.4. Receiver Collision

4.2. 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.

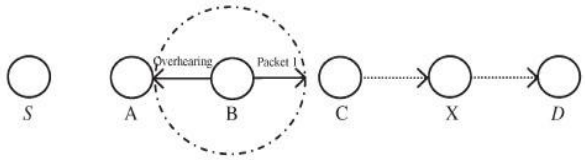

Figure.5. Limited Transmission Power

4.3. False Misbehavior Report

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

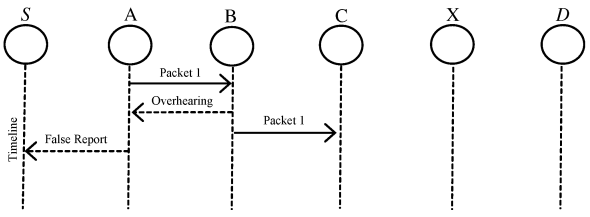

Figure.6. False Misbehavior Report

V. PROPOSED SYSTEM

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely 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, digital signature is used in this 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. In EAACK, we use 2 b of the 6 b to flag different types of packets. Fig. 9 presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

5.1. 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. 7, 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.

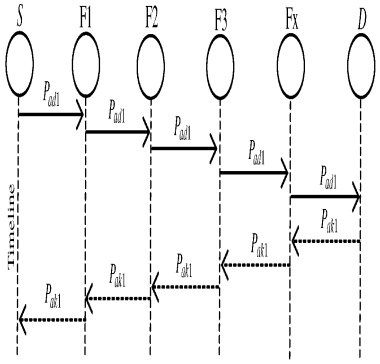

Figure.7. ACK Mode

5.2. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [16]. 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. As shown in Fig. 8, in S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet Psad1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. 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.

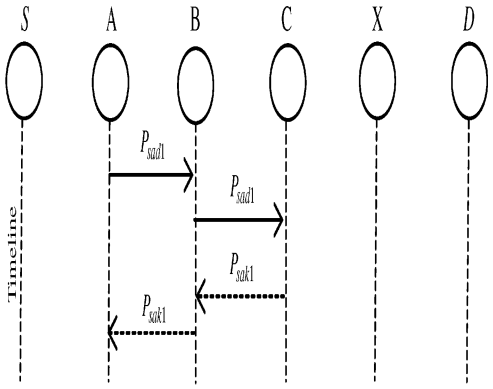

Figure.8. S-ACK Mode

5.3. 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 report innocent 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 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. 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.

5.4. 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 all rely 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 [33] and RSA [23] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

VI. MODIFICATION

The normal EAACK scheme with digital signature incorporated some network overhead mainly digital signature using RSA scheme. When hybrid cryptographic techniques are used network overhead is reduced. ECC(Elliptic Curve Cryptography) and AES(Advanced Encryption Standard)-

128 is used here. Acknowledgment packets are encrypted using AES and the key used for AES encryption is again encrypted using ECC .AES+ECC is used to reduce the packet size hence reducing overhead.

VII. ALGORITHM USED IN THE PROPOSED SYSTEM AND MODIFICATION

In this paper, mainly two algorithms are used DSA and RSA. For modification purpose, AES and ECC algorithm is used for encryption and decryption.

7.1. Algorithm 1: DSA

The DSA signature scheme is shown below.

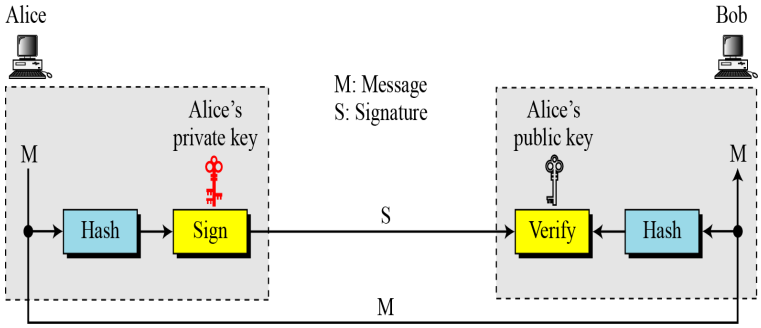

Figure.9. DSA-Signing The Digest

7.2. Algorithm 2: RSA

The key generation in RSA digital signature scheme is same as that of RSA scheme. Like in RSA scheme 'd' is kept private and both 'e' and 'n' are public.The scheme is shown below.

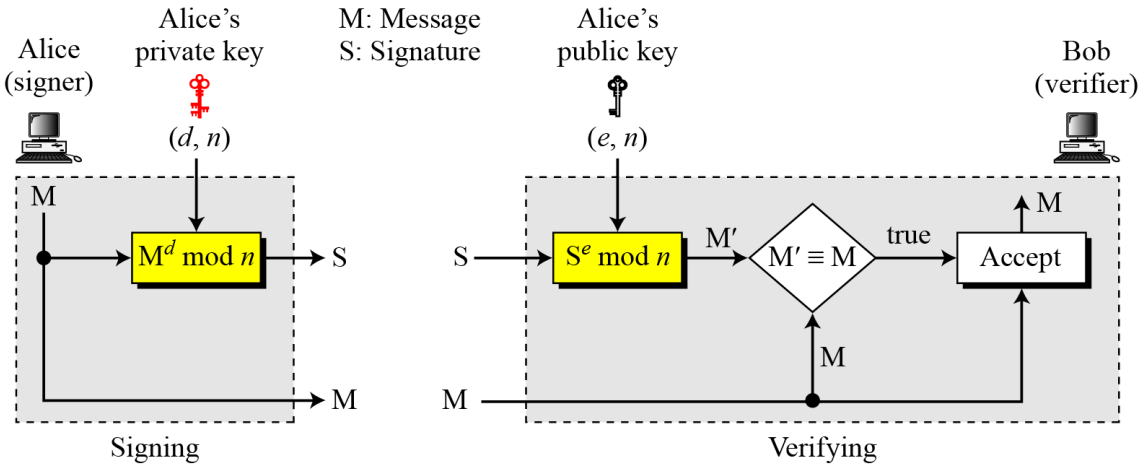

Figure.10. RSA Digital Signature Scheme

7.3. Algorithm 3: AES

The AES is a Federal Information Processing Standard, (FIPS), which is a cryptographic algorithm that is used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt, (encipher), and decrypt, (decipher), information. The key length used is 128 bits or 16 bytes. Here AES-128 is used.The key array matrix is 4x4 matrix. The encryption consists of 10

rounds. The first 9 rounds consist of 4 distinct transformation functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The final round contains only three transformations, and there is a initial single transformation (AddRoundKey) before the first round, which can be considered as Round 0. Each transformation takes one 4X4 matrix as input and produces a 4X4 matrix as output. Also, the key expansion function generates 11 round keys, each of which is a 4X4 distinct matrix. Each round key serve as one of the inputs to the AddRoundKey transformation in each round. The key expansion function expands the 128 bit key into 44 words (or 176 bytes) and thus, generates 11 round keys, each of which is a 4X4 distinct matrix.

7.4. Algorithm 4: ECC

Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA, Rabin, and El Gamal. Every user has a public and a private key. Public key is used for encryption/signature verification. Private key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems such as Elliptic Curve Diffie-Hellman Key Exchange, Elliptic Curve Digital Signature Algorithm

VIII. PERFORMANCE EVALUATION

In order to measure and compare the performances of proposed scheme, two performance metrics are adopted.

1) Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2) Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA]. During the simulation, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

To better investigate the performance of EAACK under different types of attacks, three scenario settings are made to simulate different types of attacks.

Scenario 1: In this scenario, simulated a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is used to test the IDSs' performances when the attackers are smart enough to forge acknowledgment packets and claiming positive result while, in fact, it is negative.

IX. SIMULATION

The simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. In order to better compare simulation results with research works the default scenario settings in NS 2.34 is adopted.. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. Here,ten nodes are used. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer

are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, network scenario is run three times and calculated the average performance

X. EXPERIMENTAL RESULTS

The proposed method is an experiment through NS2.The results of the proposed system shows that when scenario 1 is simulated, TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. In the second scenario, when malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%.In scenario 3 also, Eaack outperforms all the other schemes in the terms of PDR and RO. But due to the incorporation of digital signature there is some network overhead in the system. This is furthur reduced when hybrid cryptographic techniques are used. In the modification simulation, results shows that EAACK using AES and ECC reduced network overhead in all the three scenarios and outperformed the other acknowledgment based schemes including EAACK.

XI. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. Designed a novel IDS named EAACK protocol specially dsigned 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, digital signature is incorporated. Although it generates more ROs in some cases, as shown in the simulation results, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.. In order to seek the optimal DSAs in MANETs, both DSA and RSA schemes is implemented in this simulation and arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs after seeing the simulation results. As modification ,hybrid cryptographic techniques are implemented i.e., AES(Advanced Encryption Standard) is used along with ECC(Elliptical Curve Cryptography). After simulation, it is seen that network overhead is furthur reduced.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs*", IEEE Trans. on industrial electronics*, vol. 60, no. 3, march 2013.
[2] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: SpringerVerlag, 2008.
[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] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[5] 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.
[6] 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.
[7] 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.
[8] A.Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
[9] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information 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.
[10] Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[11] 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.