International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

INTRUSION DETECTION SYSTEM FOR MANETs

[1]Ms.S.P.Nandhini Priya, [2]Mrs.T.Manjula, [3]Mr.B.Anand

1. *PG Scholar, Hindusthan College of Engineering and Technology, Coimbatore.*
2. *Assistant Professor (EEE), Hindusthan College of Engineering and Technology, Coimbatore.*
3. *Associate Professor (EEE), Hindusthan College of Engineering and Technology, Coimbatore.*

Abstract— The colonization from wired network to wireless network has been a global trend in the past few years. The wireless network is possible in many applications due to mobility and scalability. MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. If the nodes are within the communication range, they can communicate directly with each other. Otherwise, they deliver on their neighbours to relay messages. The self-configuring ability of nodes in MANET made it popular among necessary 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 acute to develop efficient intrusion-detection mechanisms to preserve MANET from attacks. To improve the technology and break in hardware costs, we are expanding MANETs into industrial applications. To alter this, we strongly claim that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Secure Enhanced Adaptive Acknowledgment (SEAACK) specially designed for MANETs. Compared to contemporary approaches, SEAACK demonstrates higher malicious behaviour detection rates in certain circumstances while does not greatly affect the network performances. The SEAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different models through simulations. The results demonstrated positive performances against ACK, S-ACK and MRA in the cases of ambiguous collision, partial dropping and collusion

***Index Terms*—**Secure Enhanced Adaptive ACKnowledgment (SEAACK), Mobile Ad hoc NETwork (MANET), Acknowledgment (ACK), secure ACK (S-ACK), Misbehaviour Report Authentication (MRA).

1. INTRODUCTION

Wireless networks are preferred due to their natural mobility and scalability. Owing to the enhanced technology and lessened expenses, wireless networks have picked up substantially more inclination over wired systems in the past few decades.

By definition, Mobile Ad hoc Network (MANET) is an accumulation of versatile nodes outfitted with both a remote transmitter and a collector that speak with one another by means of bidirectional remote connections. One of the real points of interest of remote systems is its capability to permit information correspondence between diverse gatherings and still keep up their versatility. MANET allowing intermediate parties to relay data transmissions. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [6], [13]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [1], [12]. 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. In particular, 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 [4], 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. Many research efforts have been devoted to such research topics [1]-[4],[6]-[8],[13]

.

II. BACKGROUND

A IDS in MANETs

As talked about in the recent past, because of the impediments of most MANET steering conventions, nodes in MANETs expect that different nodes dependably participate with one another to transfer information. This presumption leaves the assaulters with the chances to attain huge effect on the system with only one or two traded off nodes. To address this issue, an IDS ought to be added to upgrade the security level of MANETs. Assuming that MANET can identify the assailants when they enter the system, we will have the capacity to totally dispense with the potential harms created by traded off hubs at the first run through. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [7]. Anantvalee and Wu [3] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [10], TWOACK and Adaptive ACKnowledgment (AACK) [9].

1) Watchdog: Marti *et al.* [10] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. Indeed, the Watchdog plan is comprised of two parts, in particular, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is answerable for locating malignant node mischievous activities in the system. Watchdog catches vindictive mischievous activities by indiscriminately listening to its next jump's transmission. In the event that a Watchdog node catches that its next node neglects to advance the bundle inside a certain time of time, it builds its failure counter. The point when ever a hub's failure counter surpasses a predefined limit, the Watchdog hub reports it as acting mischievously. Hence, the Pathrater participates with the steering conventions to evade the reported hubs in future transmission.

Numerous accompanying exploration studies and usage have demonstrated that the Watchdog plan is efficient. Besides, contrasted with some different plans, Watchdog is fit for recognizing pernicious hubs instead of connections. These focal points have made the Watchdog conspire a famous decision in the field. Nevertheless, as pointed out by Marti *et al.* [10], the Watchdog scheme 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. 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.* [9] is one of the most important approaches among them. On the in spite of numerous different plans, TWOACK is not an upgrade or a Watchdog-based plan. Expecting to intention the collector crash and constrained transmission power issues of Watchdog, TWOACK discovers getting rowdy connections by recognizing each information bundle transmitted over every three sequential hubs along the way from the source to the destination. Upon recovery of a parcel, every hub along the way is obliged to send back an affirmation bundle to the hub that is two jumps far from it down the way. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [7]. 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.

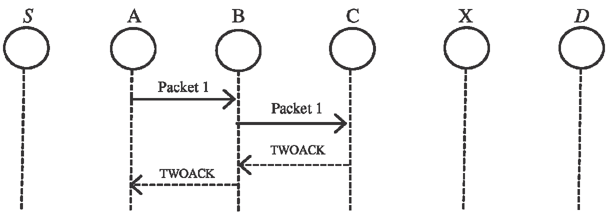

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

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: Contrasted with TWOACK, AACK fundamentally lessened system overhead while still equipped for supporting or actually surpassing the same system throughput. The finish to-end affirmation plot in ACK is demonstrated in Fig. 2. In the ACK plan indicated in Fig. 2, the source hub S conveys Packet 1 without any overhead with the exception of 2 b of banner demonstrating the bundle sort. All the moderate hubs basically send this bundle. The point when the end hub D gets Packet 1, it is obliged to send back an ACK affirmation bundle to the source hub S along the converse request of the same way. Inside a predefined time period, if the source hub S gains this ACK affirmation bundle, then the parcel transmission from hub S to hub D is great. Overall, the source hub S will switch to TACK conspire by conveying a TACK parcel. The idea of receiving a half and half plan in AACK incredibly decreases the system overhead, however both TWOACK and AACK still experience the ill effects of the issue that they neglect to distinguish malignant hubs with the vicinity of false trouble making report and fashioned affirmation parcels.

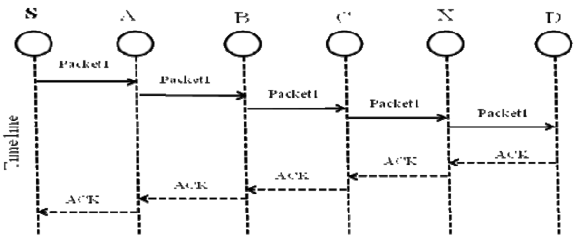

Fig.2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

In fact, many of the existing IDSs in MANETs adopt acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

B. Digital Signature

Digital signatures have dependably been an essential a piece of cryptography ever. Cryptography is the investigation of scientific methods identified with parts of data security, for example, secrecy, information trustworthiness, element confirmation, and information root verification. The security in MANETs is characterized as a blending of procedures, techniques, and frameworks used to guarantee classifiedness, validation, uprightness, accessibility, and nonrepudiation. Computerized mark is a broadly received methodology to guarantee the validation, honesty, 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 [14].

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) [14].

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 [15].

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. First, a fixed-length message digest is computed through a preagreed hash function H for every message m. This process can be described as

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

Second the sender Alice needs to apply its own private key $P_{r-Alice}$ 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

$$S_{P_{r-Alice}}(d) = Sig_{\text{Alice}}. \quad (2)$$

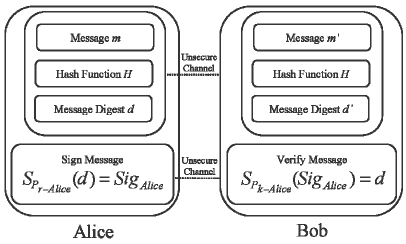

Fig.3. Communication with digital signature.

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $P_{r-Alice}$ 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.

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 against the preagreed hash function H to get the message digest d. This process can be generalized as

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

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

III. PROBLEM DEFINITION

Our proposed approach SEAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, ambiguous collisions, collusion and partial dropping. In this section, we discuss these three weaknesses in detail.

In a typical example of ambiguous 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 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.

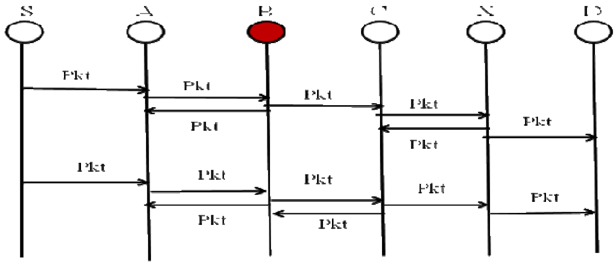

Fig. 4. Ambiguous collisions: Node B get congested due to more packet transmission at the same time.

In the case of partial dropping, in order to preserve its own battery resources, intermediate nodes intentionally limits its transmission power so that it is not strong enough to be reach node D with exact packet at sender side, as shown in Fig. 5.

For collusion, node A and node X act as a malicious node and sends a wrong packet to node B, 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 collusion attack.

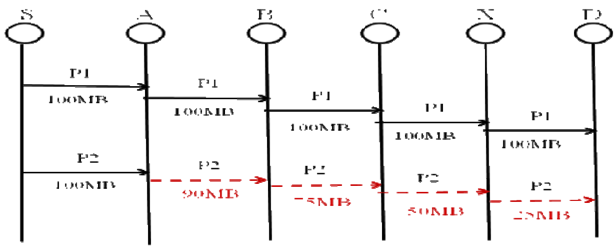

Fig. 5. Partial dropping: Intermediate nodes in net-work dropping the packet.

As discussed in previous sections, EEAACK solve two of these three weaknesses, namely, ambiguous collision and partial dropping. However, both of them are vulnerable to the collusion attack. In this research work, our goal is to propose new IDS specially designed for MANETs, which solves not only ambiguous collision and partial dropping but also the collusion problem.

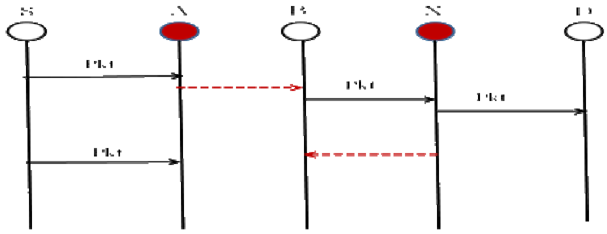

Fig.6. Collusion: Node A and X act as a misbehavior node and sends wrong packet to node B

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.

TABEL I
PACKET TYPE INDICATORS

Packet Type	Packet Flag
General Data	00
ACK	01
S-ACK	10
MRA	11

Table: 3.1 Performance result of different method

IV. SCHEME DESCRIPTION

In this section, we describe our proposed SEAACK scheme in detail. The approach described in this research paper is based on our previous work [8], where the backbone of SEAACK 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.

SEAACK is consisted of two major parts, namely, Energy based EAACK (EEAACK) and CNDA. It includes the EAACK scheme too. In order to distinguish different packet types in different schemes, we included a 2-b packet header in SEAACK. According to the Internet draft of DSR [7], there is 6 b reserved in the DSR header. In SEAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I. 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.

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. 7, 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.

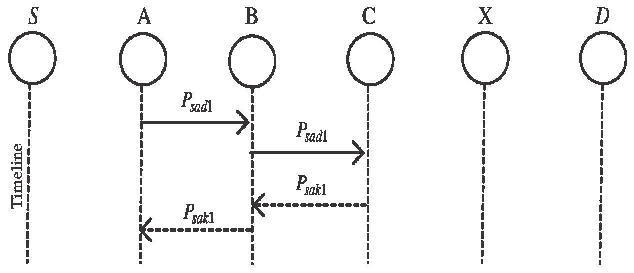

Fig.7. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [14]. 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 P_{sad1} to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives P_{sad1}, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet P_{sak1} to node F2. Node F2 forwards P_{sak1} 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.

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 report innocent nodes as malicious. 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. 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. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and un- tainted. 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 [26] and RSA [19] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

E. Energy based EAACK

The Energy based Enhanced Adaptive Acknowledgement Scheme (EEAACK) resolves two problems of watchdog such as Partial dropping and Ambiguous collisions by monitoring the Energy of all nodes which are in the network. Energy is the main problem in networks. The threshold value is fixed to each and every sensor. The sensor will be reconfigured when the energy reduces its threshold.

F. CNDA

Monitoring device is fixed in the network to detect the colluder node. If the collusion node is present it will be detected by the CNDA monitoring node

G. AODV

AODV is a method of routing messages between mobile computers. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in routes and can create new routes if there is an error.

AODV Characteristics:

✓ Will find routes only as needed
✓ Use of Sequence numbers to track accuracy of information
✓ Only keeps track of next hop for a route instead of the entire

V .PERFORMANCE METRICS

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

A. Simulation Methodologies

To better investigate the performance of SEAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: In this scenario, we 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. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform and Ubuntu 10.04. The system is running on a laptop with Intel Pentium IV CPU and 4-GB RAM In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. In NS 2.34, the default configuration specifies 42 nodes in a flat space with a size of 1000×1000 m. 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.

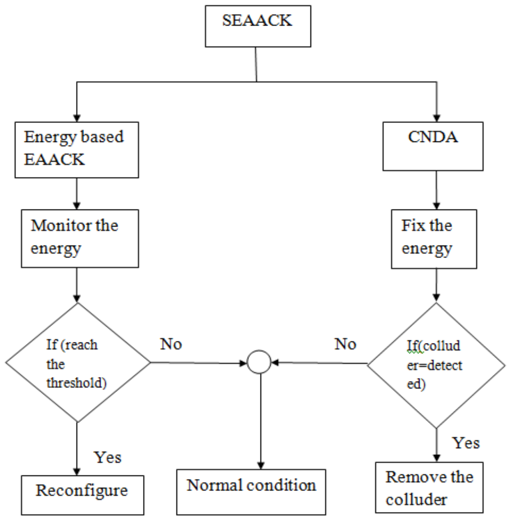

Fig. 8. S E A A C K scheme: Node C is required to send back an acknowledgment packet to node A.

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics.

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.

Regarding the digital signature schemes, we adopted an open source library named Botan [14]. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA and RSA schemes, we generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. We assumed that both a public key and a private key are generated for each node and they were all distributed in advance.

On the other hand, the sizes of public- and private-key files for 1024-b RSA are 272 and 916 B, respectively.

C. Performance Evaluation

To provide readers with a better insight on our simulation results, detailed simulation data are presented in Table II.

TABEL II
COMPARISON OF DIFFERENT METHODS

Scenario : Packet Delivery Ratio						
Methods	**Number of malicious nodes**					
	0%	**1%**	**2%**	**3%**	**4%**	**5%**
Watch dog	650	0	0	190	0	200
TWO ACK	555	0	0	188	70	140
EAACK	190	190	155	240	420	100
SEAACK	200	210	195	270	450	130

Scenario : Routing Overhead					
Methods	**Number of malicious nodes**				
	0%	**5%**	**10%**	**15%**	**20%**
Watch dog	0.79	0.96	0.56	0.38	0.54
TWO ACK	0.23	0.05	0.04	0.08	0
EAACK	0.05	0.13	0.01	0.05	0
SEAACK	0.2	0.09	0.05	0	0

Table: 5.1 Performance result of different method

1) Simulation Results—Scenario 1: In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 10 shows the simulation results that are based on PDR. In Fig. 9, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme SEAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network.

From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK.

The simulation results of RO in scenario 1 are shown in Fig. 10. We observe that DSR and Watchdog scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors. For the rest of the IDSs, AACK has the lowest overhead. Although SEAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases.

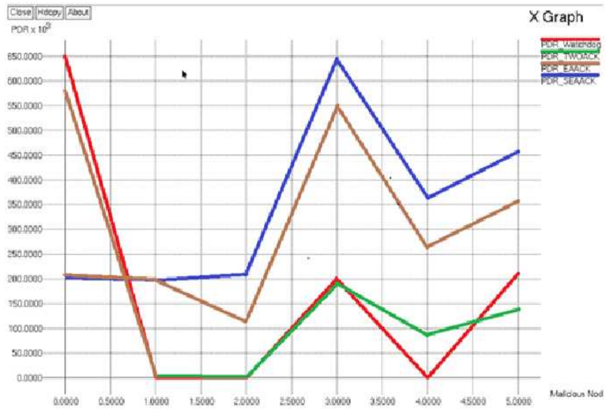

Fig: 9. Packet Delivery Ratio Vs Malicious nodes - Compared

2) DSA and RSA: In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

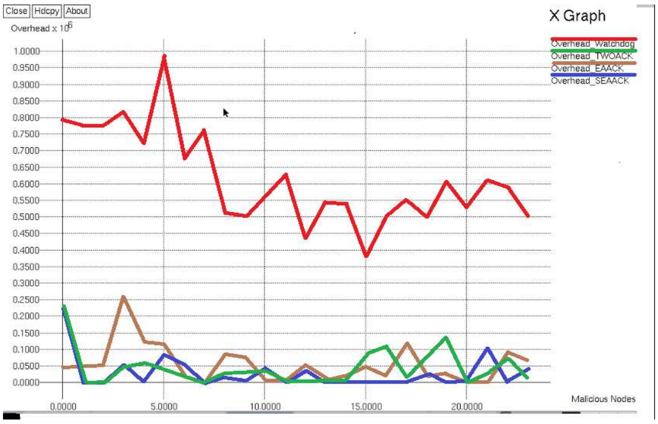

Fig: 10. Routing Overhead Vs Malicious nodes - Compared

VI. CONCLUSIONS AND FUTURE ENHANCEMENT

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 SEAACK 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 EAACK in the cases of partial dropping, ambiguous collision, and collusion.

In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs[15].

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, pp. 4266–4278, Oct. 2009.*

[2] 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.

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

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[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.

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

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

[14] 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.

[15] Botan A friendly C ++ crypto library [online] available: http ://botan.randombit.net/

[16] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

S.P.Nandhini Priya obtained her B.E. in Electronics and Communication Engineering (Anna university of Chennai, 2012), M.E. in Applied Electronics (Anna university of Chennai, 2014).She is currently doing her project work on ad hoc networks which includes security.

T.Manjula obtained her B.E. in Electrical and Electronics Engineering (Bharathiyar University, 2004), M.E in Applied Electronics (PSG college of Technology, Coimbatore, 2009).At present working in Hindustan College of Engineering and Technology with the experience of 8 years. Her area of interest is wireless and embedded system.

Dr.B.Anand obtained his B.E & M.E from Annamalai University; chithamparam.He has served as a associate professor for 11 years in Hindusthan College of Engineering and Technology, Coimbatore. His area of interest is embedded system.