Secure Performance of Intrusion Detection System for MANETs Using New Digital Signature

U. Srilakshmi
Department of Computer Science & Engineering
Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

Dr. Bandla Srinivasa Rao
Department of Computer Science & Engineering
Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

Abstract- A Mobile Ad Hoc Network (MANET) is a collection of nodes that are configured automatically without having a fixed infrastructure. Since the nodes in MANET are resource constrained the network is vulnerable to various kinds of attacks. Due to the ubiquitous nature of the network it is widely used in real world applications. Real world applications are switching from traditional networks to MANETs due to the utility of such network. Moreover MANET can be used in case of emergencies where fixed infrastructure networks are not available. Securing MANET communications is to be given paramount importance. The nodes in MANET play two roles such as transmitter and receiver. Intrusion detection system plays a vital role in protecting MANET communications. Many IDSs came into existence. However, they can be further improved. Recently Shakshuki et al. proposed EAACK that is an IDS based on acknowledgement in this paper we propose and implement an IDS that provides fool proof security to MANET besides improving in packet delivery ratio, delay and routing performance. Our simulations using NS2 revealed that the proposed IDS can secure MANET communications.

Keywords – Security, Mobile Ad Hoc Network (MANET), intrusion detection

I. INTRODUCTION

Over few decades wireless networks are preferred to wire counterparts as they are equipped with modern technologies and reduced costs besides features such as mobility and scalability. MANETs do not need infrastructure with self-configured nodes suitable for emergency operations like natural and man-made calamities, wars between countries, fire mishaps with high causality etc. [1], [2]. MANET has other features such as distributed architecture and changing topology. With such unique features this network is widely used among industries [3]. Nevertheless, MANET nodes are vulnerable to different types of attacks due to lack of physical protection. Moreover routing protocols in MANET believe that the nodes in the network are genuine with cooperative behaviour. However, adversaries are capable of inserting malicious nodes into MANET due to lack of centralized monitoring available with traditional networks. This is the reason that is why IDS plays a paramount role in MANET security.

Many solutions came into existence to protect MANET communications. Our contributions in this paper are as follows.

- We investigated MANET security and reviewed some IDS mechanisms.
- We proposed and implemented IDS that secures communications in MANET.
- We made extensive simulations that demonstrate the proof of concept.
- The remainder of this chapter is structured as follows. Section II review related literature. Section III presents the proposed a new IDS scheme. Section IV presents simulation results while section V concludes the paper besides providing directions for future work.

II. RELATED WORKS

MANET routing protocols assume that the nodes in MANET cooperate with each other. This assumption lets adversaries exploit vulnerabilities of MANET to launch various attacks. To address this issues MANET communications are secured using an intrusion detection system that can eliminate potential risks caused by the

nodes which are compromised and used as vehicle for making attacks. This section reviews literature on IDS in MANETs. Especially our work is closely related to the IDS such as Watchdog [4], TWOACK [5], AACK [6], EAACK (DSA) , EAACK (RSA) , and A3ACKs [6] in one way or other.

A. Watchdog

It was proposed in [4] which improved throughput in MANET besides securing communications. It has two parts namely Watchdog and Pathrater. The former serves as an IDS while the latter is meant for helping routing protocols for tracing misbehaved nodes and avoids them in future transmissions. The IDS part of Watchdog overhears next hop's transmission. If the next hop is not able to transmit data in certain time, it maintains a failure counter. Based on the pre-defined threshold the node which fails to forward packets repeatedly the node is deemed to be misbehaving node. Watchdog is capable of detecting malicious nodes but not the links. However, in the presence of the ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping the Watchdog cannot detect malicious nodes in MANET. To overcome these drawbacks many IDS schemes came into existence [7], [8].

DRAWBACKS OF WATCHDOG

The three important watchdog limitations in detecting malicious nodes are in the presence of receiver collision, limited transmission power, and false misbehavior report. These three are overcome in EAACK where was enhanced in this paper further to reduce routing overhead by implementing hybrid cryptosystems. The receiver collision occurs when two nodes simultaneously send packets to other node. When both B and X send packet 1 and packet 2 respectively to node C at the same time, it results in a problem. This problem is known as receiver collision problem. The second problem is limited transmission power. As described in Watchdog IDS, a node overhears the next hop node to know whether packet transmission is successful. To facilitate the one hop node limits its transmission power intentionally to enable the other node to overhear it at the cost of its capacity to forward it to next hop. The false misbehavior report problem occurs when node A sends a false report to sender node. This is done even though B sends packet to C successfully. It does mean that the node A is misbehaving and the IDS like Watchdog is not able to detect it. However, EAACK and our solution can detect it as well. Moreover our solution in this paper overcomes the RO problem of EAACK by using KEM. Before presenting our scheme let us have a revisit of other acknowledgement based schemes and their merits and demerits.

B. TWOACK AND AACK SCHEMES

This scheme was proposed by Liu et al. [5] which resolve two drawbacks of Watchdog such as receiver collision and limited transmission power. Unlike Watchdog [4], the TWOACK scheme detects misbehaving links. It needs acknowledgement for every packet sent over three consecutive nodes when it is in transit from source to the destination. Each node, when it retrieves a packet, should acknowledge the fact to the node that two hop away from the node down the route. Node A sends packet to node B. Then B sends it to C. When C receives packet, it is supposed to acknowledge this fact to node A by sending a TWOACK packet. This will confirm to A that the packet has reached C. If this does not happen in given time limit, both B and C are doomed to be malicious.

AACK scheme proposed by Sheltami et al. [6] on the other hand is an end to end acknowledgement scheme that increases throughput further besides reducing network overhead. It is the combination of TWOACK and ACK schemes. As can be seen in ACK scheme, it is evident that the source nodes send a packet and that reaches destination. However, the acknowledgement is from destination to the source making it an end-to-end acknowledgement. When this is done in some pre-defined time limit, the packet transmission is considered successful. If not, the scheme switches to TACK (similar to TWOACK) thus reducing network overhead. The problem with Watchdog, TACK, TWOACK, and AACK they heavily depend on acknowledgement packets for successful intrusion detection. However, they may fail when acknowledgement packets are fake due to malicious attacks launched by attackers. To overcome this problem EAACK came into existence.

III. PROPOSED SYSTEM

Shakshuki et al. proposed this scheme which makes use of digital signature besides an enhanced adaptive acknowledgement scheme. The digital signature can achieve the security features such as authentication, integrity and non-repudiation in MANETs. There are two kinds of digital signatures used in EAACK. They are namely digital signature with message recovery (RSA) and digital signature with appendix (DSA). EAACK with these two are

compared with experimental results. EAACK can solve three problems of Watchdog. They are false misbehavior, receiver collision and limited transmission power. The solution of EAACK has three parts namely ACK, secure ACK, and Misbehavior Report Authentication (MRA). EAACK uses 2-b packet header in order to distinguish various packet types. It assumes the links to be bi-directional. ACK is the end-to-end data transmission scheme while the S-ACK is an improved version of TWOACK. The working principle of S-ACK is that every three consecutive nodes work together for malicious node detection. When source node obtains misbehavior report, it trusts it simply. Here the MRA comes into picture which is meant for malicious node detection in the presence of false misbehavior report generated by attackers. To overcome the problem of false misbehavior problem source node finds an alternative route to destination and sends MRA packet to destination node. On receiving this packet, the destination node verifies whether the said packet has been received. If that is already received, the source node concludes that the misbehavior report it received was false. This proves that EAACK is able to detect malicious nodes even in the presence of false misbehaving report attacks. However, it believes the acknowledgement packets are genuine. This problem is overcome by EAACK by introducing digital signature usage into the IDS scheme. With this all packets of EAACK scheme needs to be signed digitally. As the digital signature helps in using public key cryptography, it is possible that fake acknowledgements initiated by adversaries can be detected. Based on EAACK the proposed system is built to be fool proof in providing security to MANET.

IV. EXPERIMENTS AND RESULTS

The proposed system is implemented using NS2 simulations to demonstrate the proof of concept. The experiments are made in terms of packet delivery ratio, delay analysis and performance on routing. The simulation environment is shown in Table 1.

PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	10 sec, 20 sec, 30 sec ,50sec and 60sec
Number of nodes	20,40,60,80,100,120,140 and 160
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	12 packets/sec
Protocol	AODV
Number of runs	550

Table 1. Environment used for simulations

Packet Delivery Ratio

First set of experiments are made on packet delivery ratio in the presence of malicious nodes. The packet delivery ratio in the presence of malicious nodes is influenced by the percentage of malicious nodes in the MANET. Since the malicious nodes misbehave and cause problems to the normal flow of data, the packet delivery ratio decreases. The results reveal that the proposed system has high rate of packet delivery in the presence of malicious nodes when compared with other techniques applied to MANET. When ATTACK shows least performance, the proposed system shows highest performance.

	10%	20%	30%	40%	50%
EAACK	0.95	0.92	0.75	0.82	0.78
WD	0.99	0.86	0.86	0.68	0.67
DSR	0.94	0.82	0.92	0.68	0.58
ATTACK	0.92	0.91	0.84	0.89	0.69

Table 2. Packet Delivery Ratio

As shown in Table 2, it is evident that the packet delivery ratio is affected by the percentage of malicious nodes in the network. The overall trend is that as the percentage of malicious nodes increases, the packet delivery ratio decreases. The results reveal that the proposed system outperforms other techniques.

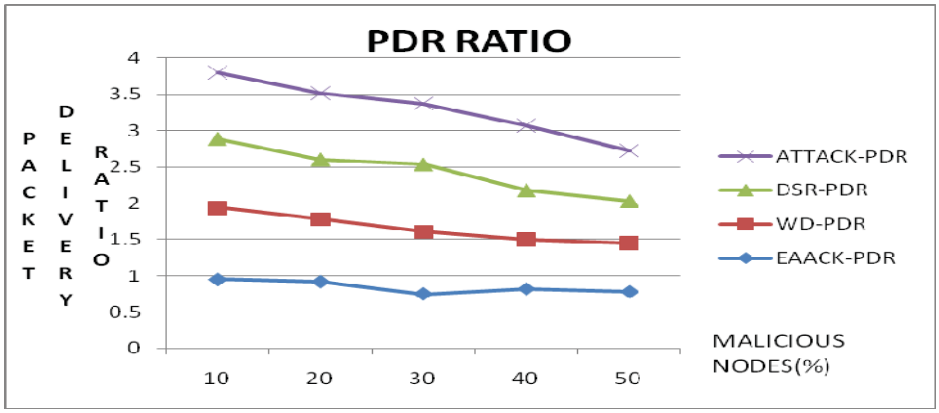

Figure 1. Comparison of performance in terms of packet deliver ratio

As seen in Figure 1, in the graph the horizontal axis represents malicious nodes' percentage while the vertical axis represents packet delivery ratio. The results reveal that the proposed method shows high packet delivery ratio in the presence of malicious nodes. However, the PDR decreases as the percentage of malicious nodes increases.

Routing Performance

	10%	20%	30%	40%	50%
WD	0.02	0.05	0.08	0.12	0.18
DSR	0.05	0.09	0.1	0.18	0.22
ATTACK	0.08	0.12	0.15	0.18	0.2
EAACK	0.01	0.05	0.09	0.14	0.18

Table 3. Routing performance

As shown in Table 3, it is evident that the routing performance is affected by the percentage of malicious nodes in the network. The overall trend is that as the percentage of malicious nodes increases, the routing performance decreases and the overhead increases. The results reveal that the proposed system outperforms other techniques.

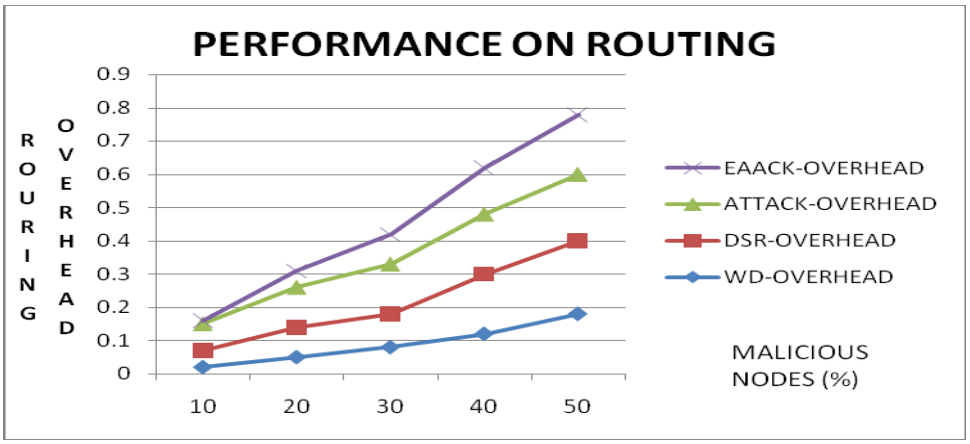

Figure 2. Comparison of routing performance

As seen in Figure 2, in the graph the horizontal axis represents malicious nodes' percentage while the vertical axis represents routing overhead. The results reveal that the proposed method shows comparatively less overhead in the presence of malicious nodes. However, the routing overhead increases as the percentage of malicious nodes increases.

Delay Performance

	10%	20%	30%	40%	50%
WD	0.2	0.4	0.8	1.2	1.5
DSR	0.1	0.3	0.6	0.9	1.3
EAACK	0.5	0.8	1.4	1.6	1.8
ATTACK	0.1	0.3	0.9	1.5	1.8

Table 4. Shows delay performance

As shown in Table 4, it is evident that the delay performance is affected by the percentage of malicious nodes in the network. The overall trend is that as the percentage of malicious nodes increases, the delay performance decreases. The results reveal that the proposed system outperforms other techniques.

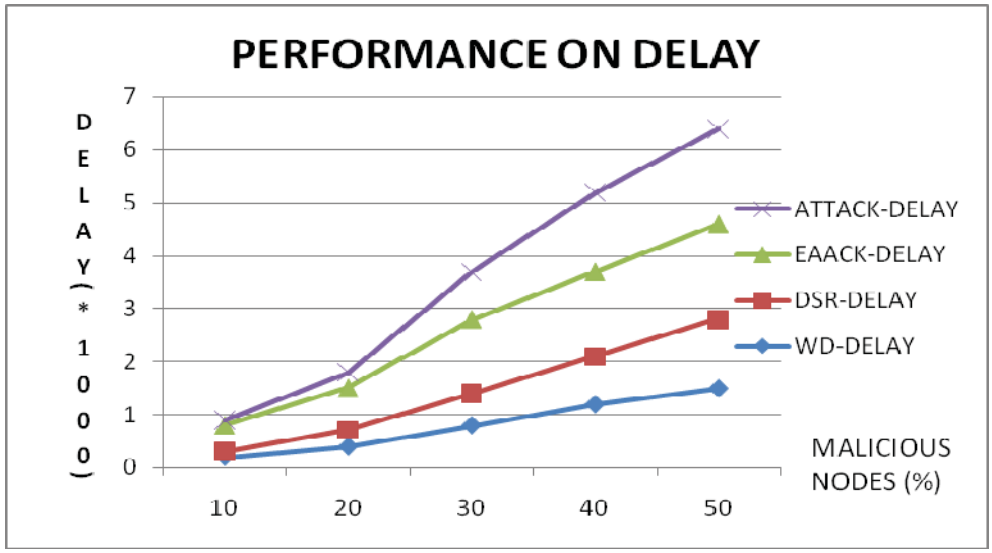

Figure 3. Comparison of delay performance

As seen in Figure 3, in the graph the horizontal axis represents malicious nodes' percentage while the vertical axis represents delay. The results reveal that the proposed method shows comparatively less in the presence of malicious nodes. However, the delay increases as the percentage of malicious nodes increases.

V. CONCLUSION AND FUTURE WORK

In this paper we studied the problem of security in MANETs. Intrusion detection is one of the counter measures for security problems in such networks. The nodes in the network are self configured and there is no fixed infrastructure available. The nodes are highly vulnerable to attacks. Traditionally intrusion detection systems were playing a major role in protecting networks. However, the traditional intrusion systems that work for wired networks are not suitable for wireless networks. Therefore it is essential to have IDS specific to MANET. Many researchers contributed towards building IDS for MANET. EAACK is one such IDS came into existence recently. In this paper we proposed and built an IDS to secure communications in MANET. Our system not only secures communications but also improves performance. In the presence of malicious nodes also, our proposed IDS performs better than existing ones. Besides improving security, our system also exhibits performance improvements in terms of packet delivery ratio, routing and delay performance. We made extensive simulations using NS2 which reveal the usefulness of our system. The empirical results are encouraging. This research can be extended further to incorporate attack models to evaluate the robustness of the proposed system.

REFERENCES

[1] 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.

[2] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting".

[3] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2003.

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

[5] 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.

[6] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds", ScienceDirect, 5th International Conference on Ambient Systems, vol. 32, pp.571-578, 2014.

[7] 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.

[8] 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.