RESEARCH ARTICLE OPEN ACCESS

Impregnable Intervention Finding System For MANETS

Beegam Chandran Srinivasan[1], K Thulasi[2]
PG Scholar[1], Associate. Professor[2],
Department of Computer Science and Engineering
Chadalawada Ramanamma Engineering College -Tirupati, Chittoor
Andhra Pradesh - India

ABSTRACT

The migration of wireless network from wired network has a global trend in the past few decades. Mobile Ad-hoc Network (MANET) technology is designed for the establishment of a wireless network anywhere, anytime without any fixed infrastructure. 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 neighbors to relay messages. The MANET is 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. An intruder can attack ad-hoc network by loading network resources such as wireless links or battery levels and by distributing the normal operations of routing protocol. So, 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, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK provides higher malicious-detection rates and does not greatly affect the network performances.

Keywords:- Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (EAACK), Mobile Ad hoc Network (MANET).

I. INTRODUCTION

Mobile Ad-hoc Network is a collection of mobile nodes equipped with both wireless transmitter and receiver that communicate with each other via bidirectional wireless links either directly or indirectly.

Fig.1 Wireless MANET

A. *Need of MANET*

The traditional wireless network communication is limited to the range of transmission. This means that two nodes cannot communicate with each other when the distance between the nodes is beyond the communication range. This problem is solved by MANET. The MANET is divided into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their range.

B. *Characteristics of MANET*

i. MANET has a decentralized network infrastructure.

ii. Manet does not require fixed infrastructure; thus all nodes are free to move randomly.

iii. MANET is capable of self-configuring and self-maintaining.

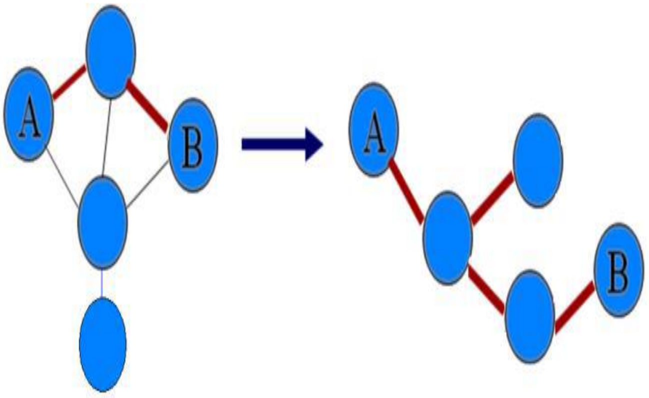

Fig.2 Topology changes frequently

C. *Security issues of MANET*

i. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.

ii. Furthermore, because of MANETs distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs.

iii. Every node in MANETs always cooperates with other nodes to data transmission. This opportunity allows the attackers to achieve significant impacts on network.

II. EXISTING SYSTEM

In MANETs, There are three Intrusion-Detection System are used in existing system namely, Watchdog, TWOACK and Adaptive ACKnowledgment (AACK).

A. Watchdog and Pathrater

The Watchdog scheme is consisted of two parts:

1.) Watchdog: It serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviour by listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving.

2.) Pathrater: It cooperates with the routing protocols to avoid the reported nodes in future transmission.

B. TWOACK

It detects misbehaving node by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. It leads to unwanted network overhead. The working process of TWOACK is shown in Fig.

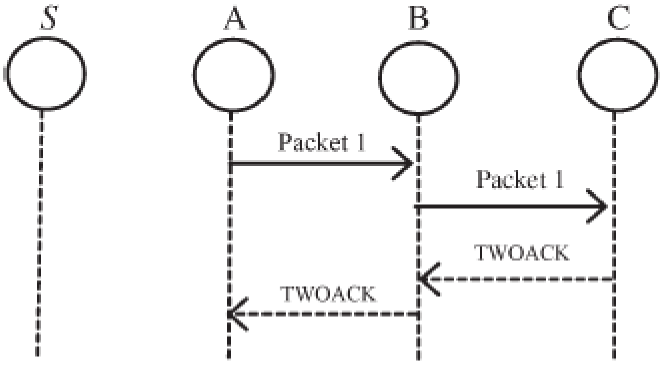

Fig.3 TWOACK Scheme

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.

C. AACK

It is a combination of a TWOACK (TACK) and an end-to-end acknowledgment scheme called ACKnowledgement (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.

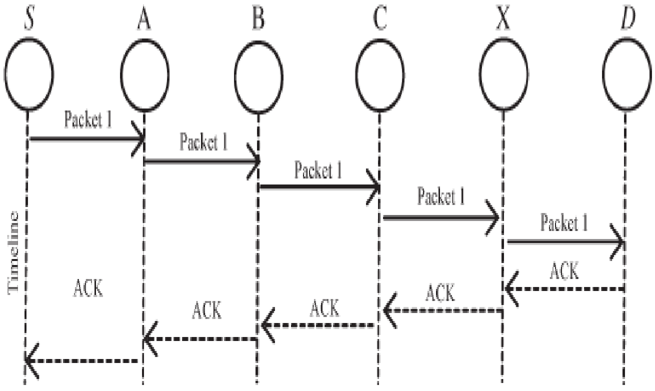

Fig.4 AACK Scheme

In the ACK scheme, all the intermediate nodes from the source node S to destination node D simply forward the packet send by source to Destination D. When the Destination D receives packets, it send back an ACKnowledgement to source S. If the source S does not receive ACK packet, then it switch to TACK scheme by sending TACK packet. This hybrid scheme reduces the network overhead.

III. DRAWBACKS OF EXISTING SYSTEM

Watchdog scheme is not effective in some situations. That is, Watchdog scheme fails to detect malicious misbehaviours with the presence of the following:

1) Ambiguous collisions
2) Receiver collisions
3) Limited transmission power
4) False misbehaviour report
5) Collusion
6) Partial dropping

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.

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 acknowledgement packets.

IV. PROBLEM DEFINITION

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

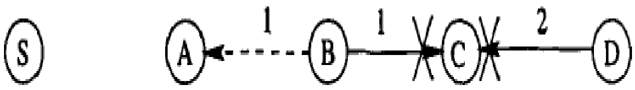

Fig. 5 Receiver Collision

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C.

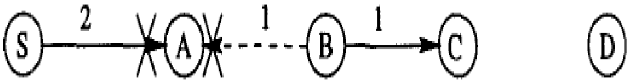

Fig. 6 Limited transmission power

For false misbehaviour report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehaviour report attack.

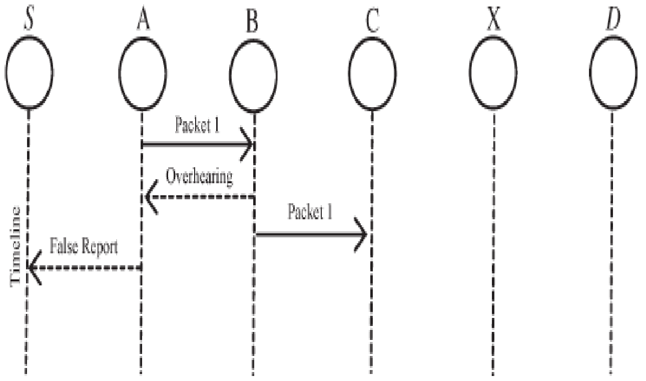

Fig. 7 False misbehaviour report

The TWOACK and AACK solve two of these three weaknesses as receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehaviour attack. So new IDS is specially designed for MANETs which solves not only receiver collision and limited transmission power but also the false misbehaviour problem.

- The existing intrusion detection system is largely depends on the acknowledgment packets. The intruder can prepare the forged acknowledgement packets. Hence it is crucial to guarantee that the acknowledgement packets are valid and authentic. Due to this digital signature is included in acknowledgement packet.
- In MANET, the attacker can make the node as malicious to send false misbehavior report. So, Misbehavior Report Authentication (MRA) should be applied.
- The key distribution in wireless Mobile Ad-hoc Network is an important issue and consumes network overhead.

V. PROPOSED SYSTEM

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). 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. 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.

A. ACK implementation

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected.

If Node A first sends data packet pak1 to destination Node D via intermediate nodes. If node D successfully receives p1, it sends back ACKnowledgement packet pak1 along the same route but in a reverse order. Within predefined time, node A receives Pak1, the packet transmission is successful. Otherwise, node A switch to S-ACK mode by sending an S-ACK data packet to detect malicious node in the route.

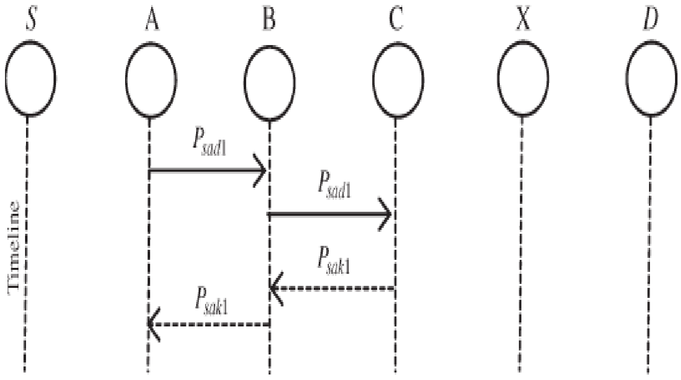

Fig. 8 ACK Scheme

B. Secure Acknowledgment (S-ACK)

It is an improved version of the TWOACK scheme. 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., 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. 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.

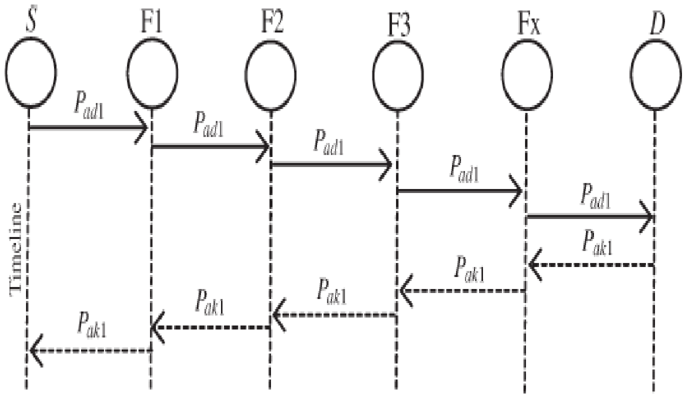

Fig.9 Secure Acknowledgment scheme

C. MRA

MRA scheme is vital to detect false misbehavior report. When MRA mode is initiated, the source node searches its local knowledge base and seeks for an alternative route to the destination node and send MRA packet.

When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet is received. If yes, we conclude that this is a false misbehavior report and whoever reported this packet is marked as malicious, otherwise the misbehavior report was trusted and accepted.

D. Digital Signature Validation

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 significant 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. EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

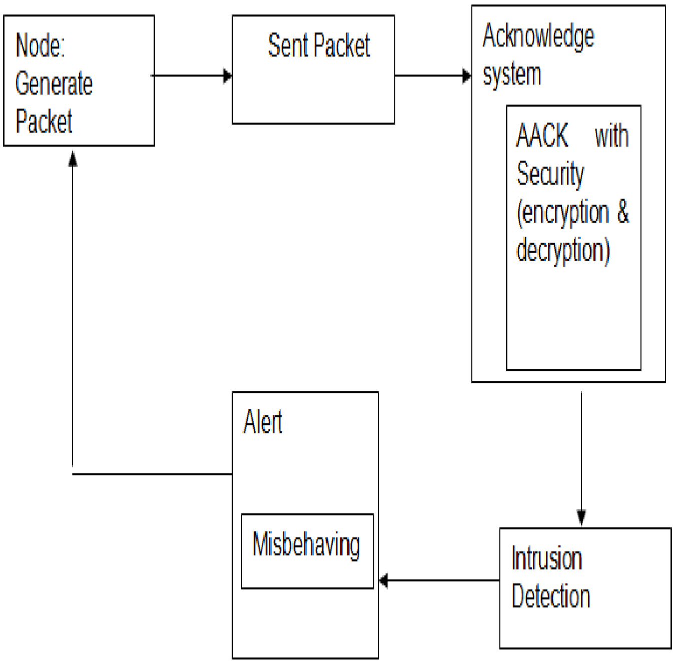

Fig. 10 Architecture Design

VI. PERFORMANCE EVALUATION

The performance of the proposed system is evaluated by comparing the simulation results of Watchdog, TWOACK and EAACK schemes.

A. Simulation Methodologies

The performance of EAACK is investigated under different types of attack. We propose three scenario settings to simulate different types of misbehaviors or attacks.

*1.) **Scenario 1:*** In this scenario, a basic packet dropping Attack is simulated. 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.

*2.) **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.

*3.) **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 with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM.

In order to measure and compare the performances of our proposed scheme, we 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].

C. Performance Evaluation

1) Simulation Results—Scenario 1: In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 11 shows the simulation results that are based on PDR. In Fig. 11, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK 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.

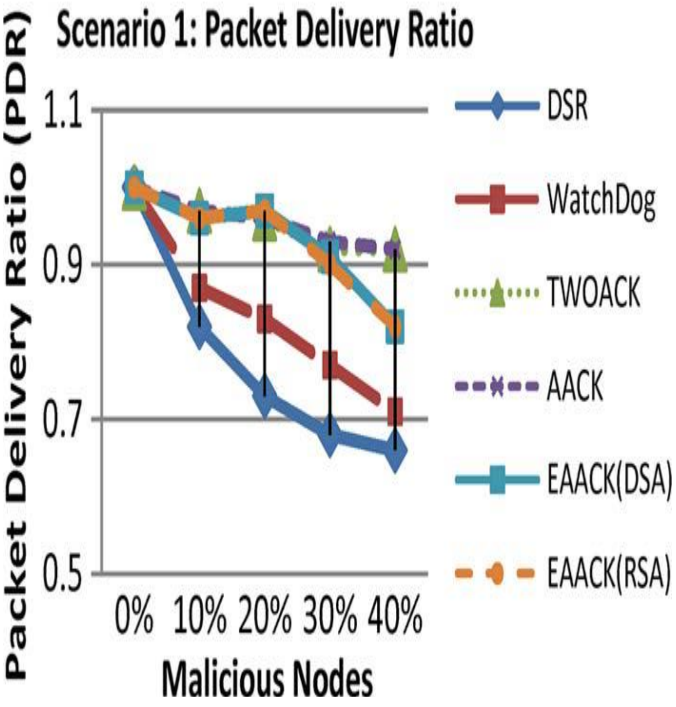

Fig. 11 Simulation results for scenario 1—PDR

The simulation results of RO in scenario 1 are shown in Fig. 12. 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.

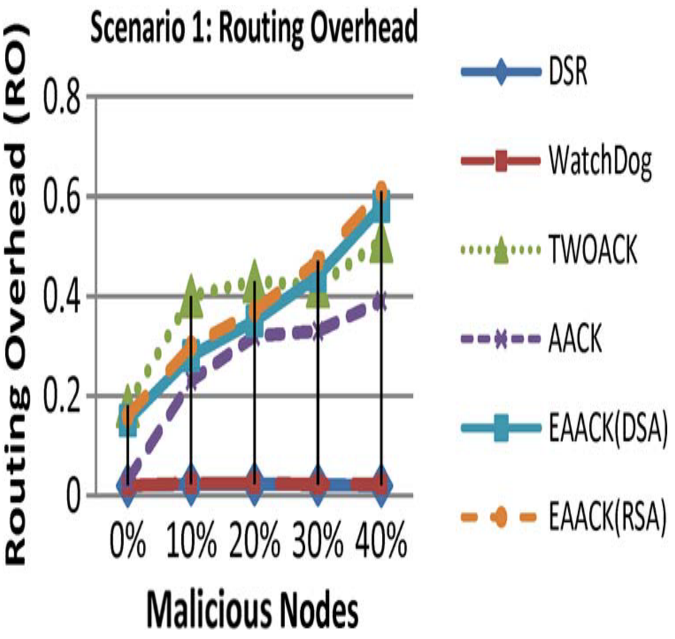

Fig. 12 Simulation results for scenario 1—RO

2) Simulation Results—Scenario 2

In the second scenario, we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report. Fig. 13 shows the achieved simulation results based on PDR.

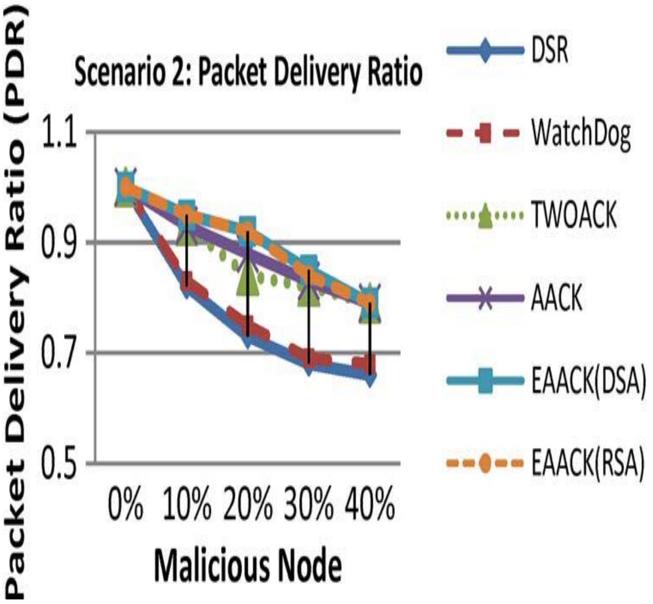

Fig. 13 Simulation results for scenario 2—PDR

In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, as shown in Fig. 14.

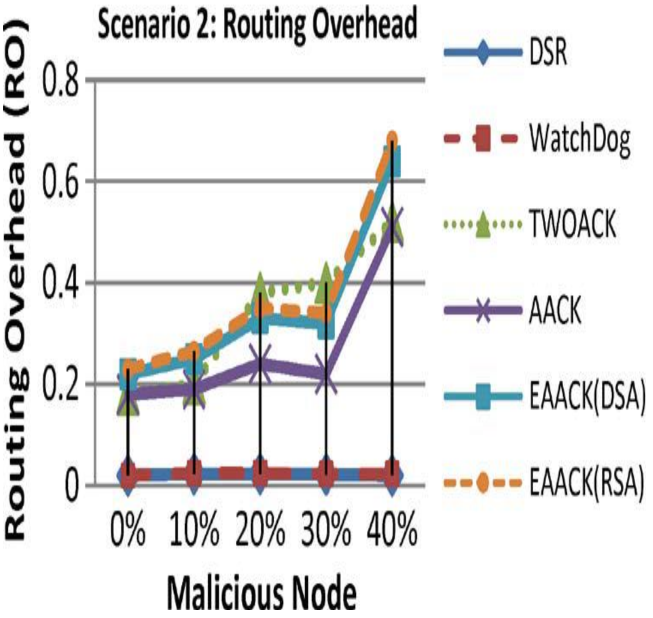

Fig.14 Simulation results for scenario 2—RO

3) Simulation Results—Scenario 3

In scenario 3, we provide the malicious nodes the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary. This is a common method for attackers to degrade network performance while still maintaining its reputation.

The PDR performance comparison in scenario 3 is shown in Fig. 15. We can observe that our proposed scheme EAACK outperforms TWOACK and AACK in all test scenarios. We believe that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets.

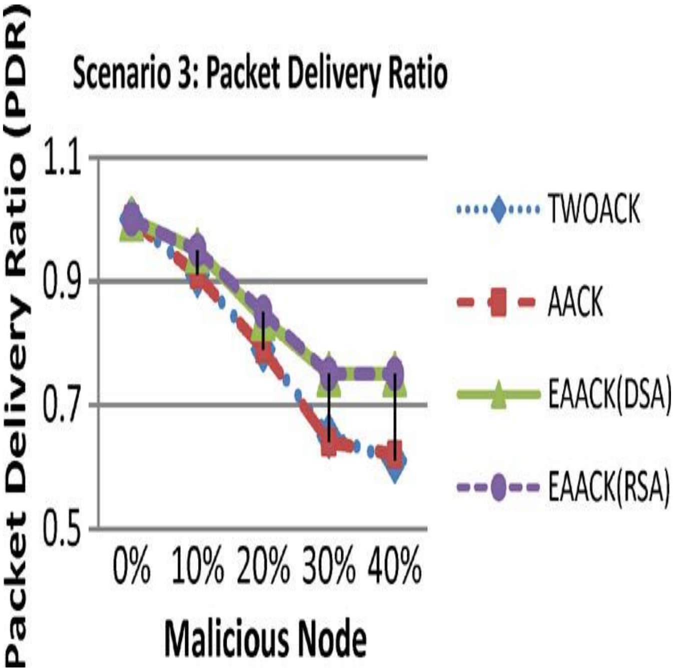

Fig. 15 Simulation results for scenario 3—PDR

Fig. 16 shows the achieved RO performance results for each IDS in scenario 3. Regardless of different digital signature schemes adopted in EAACK, it produces more network overhead than AACK and TWOACK when malicious nodes are more than 10%. We conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes.

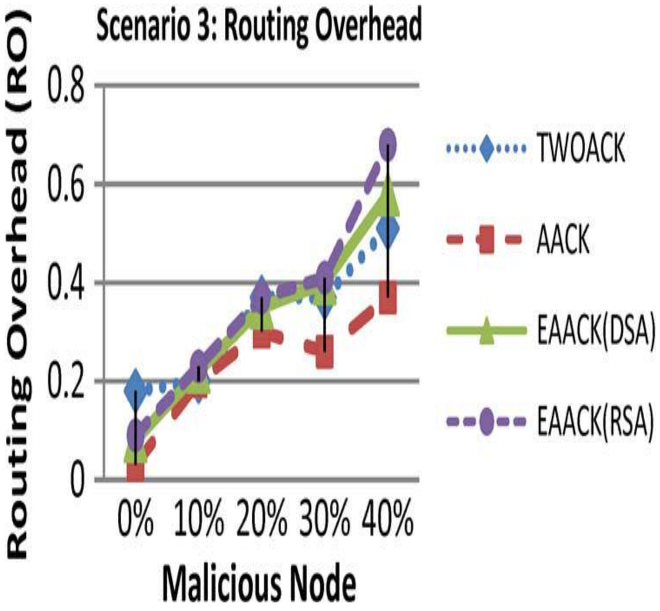

Fig. 16 Simulation results for scenario 3—RO

VII. CONCLUSIONS

Packet-dropping attack has always been a major threat to the security in MANETs. This proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report.

Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, digital signature is incorporated in our proposed scheme. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits, the following issues may be investigated in our future research:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys.

3) Testing the performance of EAACK in real network environment instead of software simulation.

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people who have made it a possibility. It is our great privilege to express our gratitude and respect to all those who have guided and inspired us to do publish this paper. We wish to express our sincere gratitude to **Prof. R. SURESH M.Tech, (Ph.D)** Head of the Department C.S.E for providing constant support.

We take this opportunity to express our sincere gratitude to my guidance **Mrs.K. THULASI M.Tech**, Assoc.Prof. Dept of C.S.E for providing her constant support throughout our project. Finally, we are very thankful to our parents, our friends and others who directly or indirectly helped us in completing this work.

REFERENCES

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: Asurvey,” 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, A. Perrig, and D. Johnson, “ARIADNE: A secure on-demand routing protocol for ad hoc networks,” in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.

[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] 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, pp. 488–494.

[10] 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.

[11] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37. Malicious nodes in mobile ad hoc network,” in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[12] 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.

[13] 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.

[14] A. Singh, M. Maheshwari, and N. Kumar, “Security and trust management in MANET,” in *Communications in Computer and Information Science*, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[15] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[16] M. Zapata and N. Asokan, “Securing *ad hoc* routing protocols,” in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[17] L. Zhou and Z. Haas, “Securing ad-hoc networks,” *IEEE Netw.*, vol. 13,
no. 6, pp. 24–30, Nov./Dec. 1999.

***K.*Thulasi** received M.Tech degree in Computer Science and Engineering from Sri Venkateswara University, Tirupati, Andhra Pradesh, India in 2006 and B.Tech degree in Computer Science and Engineering from MITS Engineering College, Andhra Pradesh, India in 2006

She is currently a Associate Professor in Chadalawada Ramanamma Engineering College, Tirupati. She published over 10 research papers in international journals, conferences, and workshops. She contributed in many international conferences and workshops with different roles.

Beegam Chandran Srinivasan pursuing M.Tech degree in Computer Science and Engineering from CR Engineering College, Tirupati, Andhra Pradesh in India. He is received B.Tech degree in Computer Science and Engineering from Seshachala Institute of Technology, Puttur, Andhra Pradesh, India in 2012.