EAACK-Intrusion-Detection-System for MANETs

Mumtaz Ahmed
Department of Computer Engineering Jamia Millia Islamia New Delhi, INDIA
ahmedmimtaz01@gmail.com

Aqib Nazir Mir
Department of Computer Engineering. Jamia Millia Islamia New Delhi, INDIA
miraqib204@gmail.com

Abstract **Future wireless communication systems will be greatly dependent on the instantaneous deployment of independent mobile users. Some of the notable and interesting examples include creating sustainable, well organized, well planned, effective, and active communication systems for emergency/exigency/crises operations, catastrophe relief efforts, and military networks. Such networking situations depend on distributed, dispersed and disorganized connectivity, and can be designed as applications of Mobile Ad Hoc networks. A MANET is a self-governing and self-organizing collection of mobile nodes with relatively equal bandwidth that communicate over restricted wireless links. A MANET network is decentralized and disseminated, where all networking including topology discovery and conveying the messages must be achieved by the nodes themselves, i.e., routing capabilities are assimilated into mobile nodes. However, determining feasible routing paths for distributing messages in a decentralized network where network topology varies is a difficult job. Factors such as the open medium and vast distribution of nodes, topological changes, variable wireless link quality, and propagation path loss become pertinent issues and make MANET unprotected to intrusions. Thus, it becomes pivotal to develop a systematic intrusion detection scheme to secure Mobile Ad Hoc networks from intruders. In this paper, we put forward and applied an efficient IDS mechanism based on Enhanced Adaptive Acknowledgment (EAACK) especially made for MANETs which performs better than the previous techniques such as Watchdog, TWOACK and AACK.**

Keywords: Mobile Ad hoc Network (MANET) Acknowledgment (ACK), Secure Acknowledgment (S-ACK), Misbehavior Report Authentication (MRA), Digital Signature Algorithm (RSA), Enhanced Adaptive Acknowledgment (EAACK).

1. Introduction

WIRELESS networking is the need of hour for many applications because of its easier network expansion, increased mobility [27] [29], improved responsiveness, better access to information, and enhanced guest access. In addition, with the increasing standard of industry and use of lightweight network hardware devices that are even smaller and largely mobile. The wireless communication is enhanced by Mobile ad hoc networks (MANETs) having high degree of node mobility.

A **Mobile Ad Hoc Network** (MANET) [28] is a self- maintaining and self- configuring network with autonomous nodes, collection of mobile nodes formed without the use of centralized infrastructure. The communication between the nodes is done with wireless transmitter and wireless receiver within the specified communication range. This means that the two nodes can communicate only if they are present in specified range. MANET [28] solves this issue by allowing the intermediate nodes to transmit data transmissions. This is attained by dividing Mobile Adhoc Networks into two types of networks, viz, single-hop and multi-hop. In a single-hop, all mobile nodes which lie in the same radio communication range transfer data directly among each other [9]. On the other side, in a multi-hop network, nodes depend on other intermediate nodes to transmit data, if destination node is beyond their radio communication range. MANETs are growing rapidly. Manets are used in various fields due to their large applications like in Military, Industrial use, civilian use. Manets can be set up without using static infrastructure or human interaction. The network topology changes frequently [29] as the mobile nodes have an important property i.e. the mobility that gives them the flexibility to move anywhere in the network or can move outside the network. This flexibility provided is useful but on the other hand makes it vulnerable to new security risks due to the cooperativeness and open broadcast medium of the mobile devices (that generally possess computational capacities and different resource, and limited battery power). As a result, intrusion detection becomes an indispensable part of security for MANETs. The intrusion detection techniques designed for traditional wired networks cannot be implemented for wireless networks due to different characteristics. Therefore, to make intrusion detection systems work effectively new techniques need to be developed for MANETs.

This paper is divided into different sections as follows. Section 2 gives brief idea on the background of intrusion

detection systems, existing techniques for intrusion detection in MANETs are presented. Some of the problems of the existing IDS for MANETs are given in Section 3. Then, our proposed EAACK scheme in Section 4, along with the simulation results. Final part explains the results and future work are discussed in section 5 and 6

2. Existing Techniques

In traditional networks many intrusion detection systems have been proposed, the routers, gateways or switches are used for network traffic. Hence, it is easy to implement IDS in these networks. In MANETs we do not use such devices. Moreover, due to its openness so both malicious and legitimate users can access. In mobile environment it is very difficult to separate normal and unusual activities. Sometimes the false routing information can be generated by outdated node or from a malicious node due to the arbitrarily movement of nodes. Thus, the available intrusion detection techniques used in simple wired networks cannot be implemented to MANETs directly. Researchers have developed many intrusion detection systems for the MANETs. In the next section, we briefly explain three existing techniques, i.e. Watchdog [17], TWOACK [34], and (AACK) [25].

2.1. WATCHDOG:

Marti et al. [17] the watchdog method was proposed to improve throughput when malicious nodes are present in network. This scheme is used as IDS in MANETs. WATCHDOG scheme is used to detect any malicious node in network. The working of WATCHDOG is divided into two parts, namely, Watchdog and Path rater. The malicious nodes are detected by listening to all nodes that lie in transmission range. WATCHDOG scheme ensures that the packet is sent to next node. If the packets are not send to next node then the node is labelled as malicious. But if match is confirmed it means packet is delivered successfully, that's results the trustworthiness of neighbor is to be incremented. If a node fails to forward the packet in a given time period, then the failure rate of a node responsible for forwarding the packet is incremented. The node is named as malicious node if the tally reaches beyond threshold value.

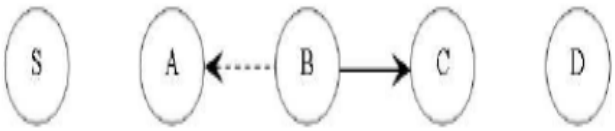


Figure 1: Shows watchdog working: Node B wants to send a packet to c, this transmission is overheard by node A.

In the Path rater scheme, every node rates the neighbors by using the information given by watchdogs. The classification of nodes like Member, Unstable, stable Suspect or malicious is done by route guard mechanism which is the combination of watchdog and Path rater. As a result, paths containing malicious nodes will be avoided. As it is clear, that the core of every type of IDS solutions for MANETS are watchdogs. The main benefits of using watchdog is that it uses local information to detect an attacker, hence avoids the role of malicious node while the decisions are made by mechanism. In comparison, the watchdog scheme suffers from a well-known drawback: it fails to detect when two nodes are consecutively attacked, it can only monitor the first node attacked while the other malicious node performs an attack.

Nevertheless, the Watchdog scheme cannot detect malicious nodes misbehavior due to the presence of the following:

1) Receiver collisions;

2) Limited transmission power;

3) False misbehavior report.

2.2. TWOACK:

To overcome the drawbacks of WATCHDOG Liu *et al.* [16] designed TWOACK scheme. The TWOACK scheme is implemented by using any source routing protocol such as DSR [11]. TWOACK is not based on WATCHDOG or enhancement based scheme. It is implemented to solve the problems like limited transmission power and receiver collision problems. This method works on the fact that the route is derived by the packet from source for a specific data packet. The acknowledgment packets used by TWOACK are known as TWOACK packets that have the fixed route of two hops in the direction opposite to data packets. When the packet is retrieved, the acknowledgment packet is sent back by every single node present on the route to the node which are two hops away from it.

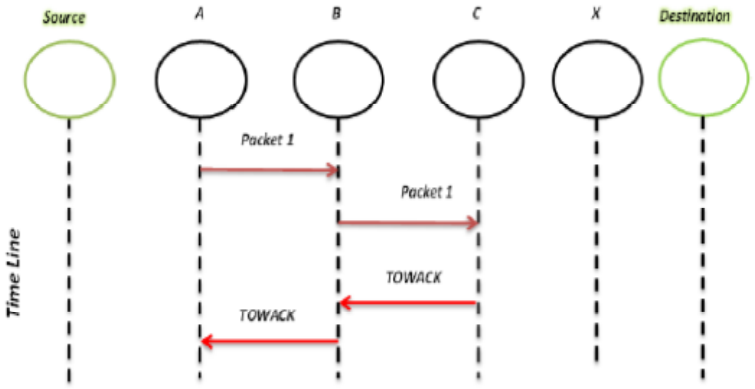


Figure 2: Working of TWO-ACK scheme:

In figure 2 a packet1 is sent to B from A and the same packet is forwarded to node C.as the C receives the packet, it generates

TWO-ACK packet as two hops are completed and sends the packet back through same route. If the packet is received in well-defined time then it is successful transmission else both the nodes C and B are tagged as malicious.

The TWOACK scheme proves successful in solving the limited transmission power [25], and receiver collision problem [28], [29]. However, the acknowledgment mechanism required in every single packet transmission added a significant amount of undesirable network overhead.

2.3. AACK:

Sheltami *et al.* [25] The problems of WATCHDOG are solved by AACK and the performance of TWOACK is improved due to reduction in routing overhead. AACK is actually combination of two namely TACK (identical to TWOACK) and ACK (end-to-end acknowledgment). The network overhead is reduced but malicious nodes with false misbehavior report and forged acknowledgment packets cannot be detected. The end-to-end acknowledgment scheme in AACK is shown in Fig. 3

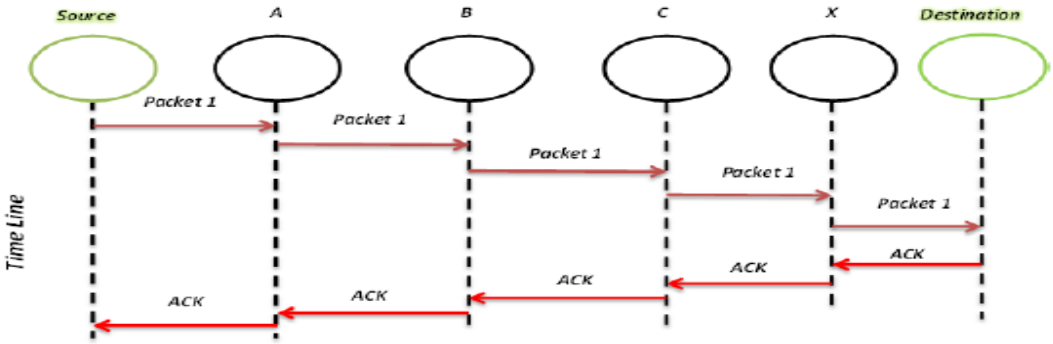


Figure 3: MANETs scheme with END TO END ACK:

The main problem still present in AACK and TWOACK is that they fail to identify malicious nodes with false misbehavior report or fake acknowledgment packets.

Hence, it is important to guarantee the authenticity and validity of acknowledgment packets are, thus the Digital Signature [18] is incorporated in our proposed scheme.

3. Problem Identification

In this section, we will highlight three major problems namely: limited transmission power, false misbehavior and receiver collision report which will be resolved by our proposed EAACK approach.

- ***Receiver collision:***

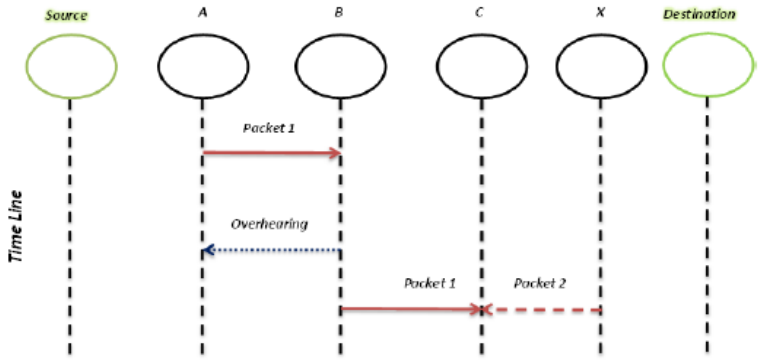


Figure 4: Receiver collisions: collision at node c due to packets sent by node B and C simultaneously.

- ***Limited power transmission:***

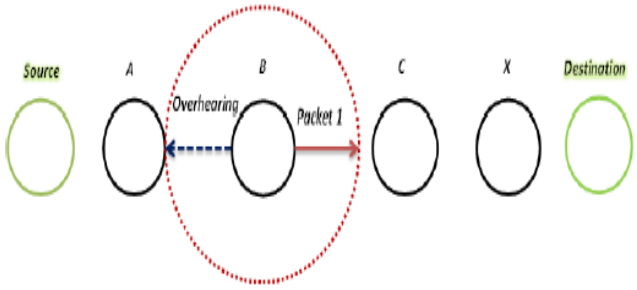


Figure 5: Limited power transmission: transmission power of node B is limited to protect overhearing but fail to reach node C.

- ***False misbehavior report:***

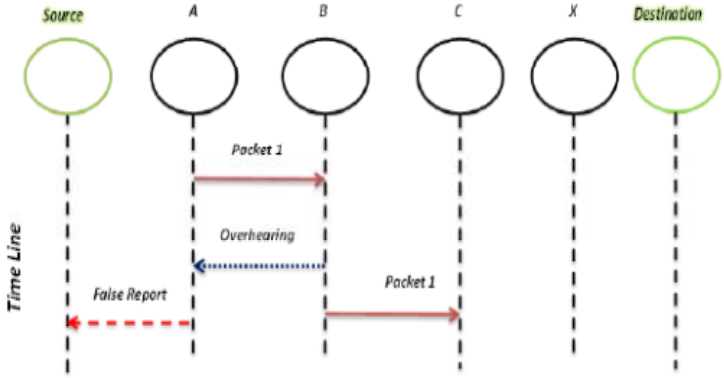


Figure 6: False misbehavior report: packet is forwarded to B but still A sends misbehavior report

4. Proposed EAACK Scheme

In this section, we are going to discuss our proposed EAACK model in detail. EAACK scheme consists mainly three major modules, namely ACK, MRA and S-ACK.

- **ACK**

It is actually an end-to-end acknowledgment scheme. It functions as a part of hybrid scheme and network overhead is reduced by using it. As in Fig. 7, node acknowledgment data packet $Pad1$ is sent out to the destination D. If the destination D receives packet successfully, it means there is no malicious node present in route. The node D sends an acknowledgment packet $Pak1$ in reverse order but along same route. If in a specified time period, packet $Pak1$ is received by source S, it means packet transmission from source to destination is successful. Otherwise, source S will use S-ACK mode to detect the malicious nodes in the route by sending S-ACK packets.

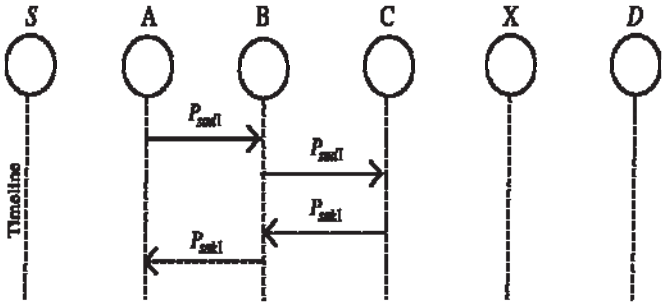


Fig. 7. ACK method: an acknowledgment packet is send by destination node after receiving a new packet.

- **S-ACK**

This is an improved version of the TWOACK scheme given by Liu *et al.* [16]. The basic principle to detect malicious nodes in network is based on fact that every three consecutive nodes in network are grouped together. In the three-node group present in the route the S-ACK acknowledgment is sent by third node to first node. The S-ACK mode is introduced to detect malicious nodes in network in presence of limited transmission power or receiver collision.

As illustrated in Fig. 8, in S-ACK mode, the group of three consecutive nodes (F1, F2, and F3) work together in order to detect any malicious nodes. The node F1 first sends out S-ACK packet $P_{sad}1$ is sent by the node F1 to the F2. Then, the packet is forwarded to node F3 from the node F2. When the packet Psad1 is received by node F3, as it is the last node in group, then node F3 sends back an S-ACK packet $P_{sak}1$ to F2 and node F2 forwards this packet to F1 node. If F1 node does not receive the acknowledgment packet on time, both the nodes F2 and F3 in group are reported as malicious nodes. Moreover, the misbehavior report is generated by F1 which is forwarded to source node S.

In the TWOACK scheme, the source node trusts immediately the misbehavior report, but in EAACK the source node requires to verify the report by switching to MRA mode. This is a very important step to detect false misbehavior report

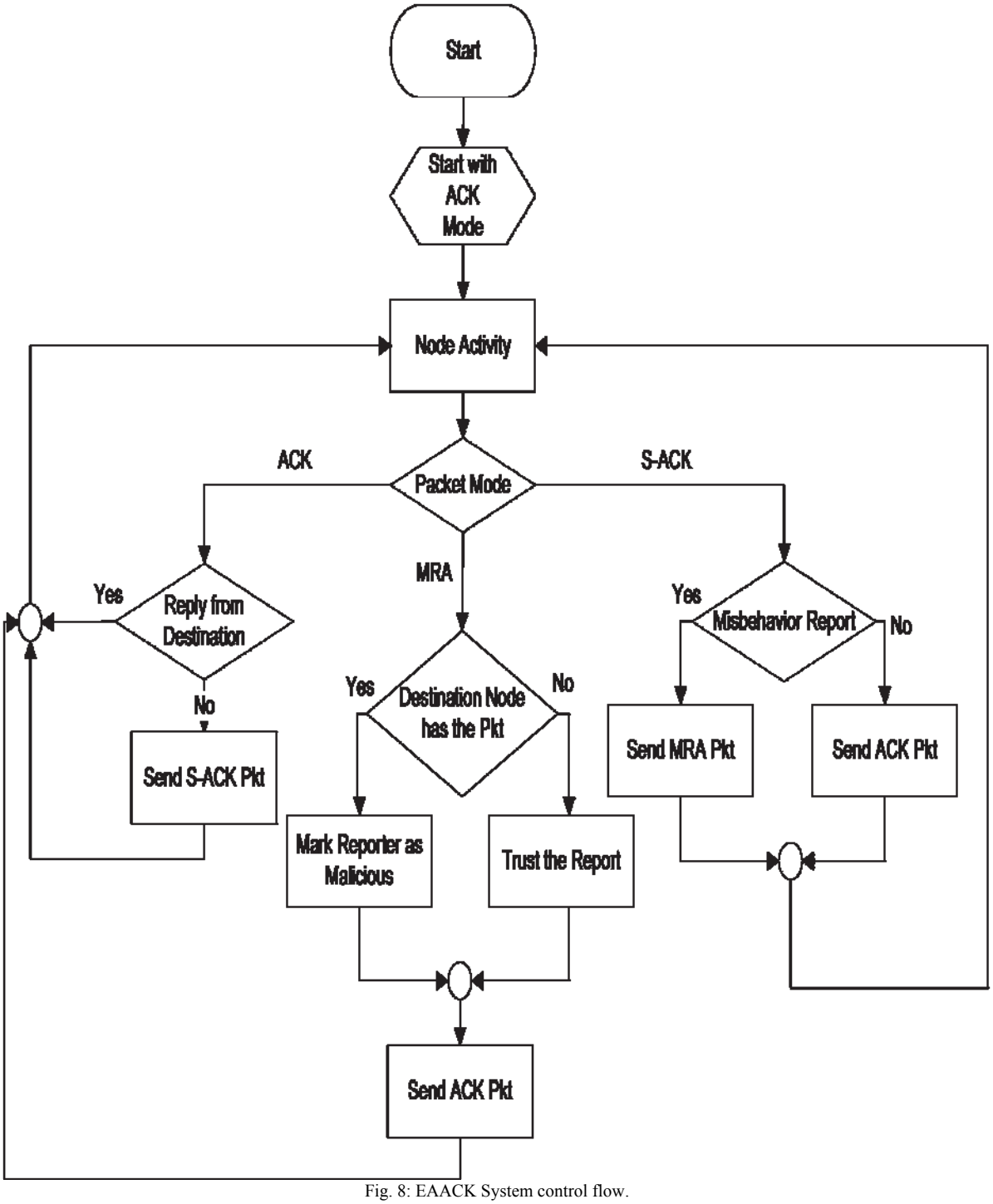


Fig. 8: EAACK System control flow.

- ***MRA***

The MRA scheme is designed to detect misbehaving nodes when a false misbehavior report is generated. In false misbehavior report the innocent nodes are represented as malicious nodes by attacker. This attack can damage the entire network and sufficient nodes can be broken down to cause a network division. The aim of MRA scheme is to authenticate the misbehavior report.

In MRA mode, the local knowledge base is searched by the source node to check for an alternative route to the destination node. If no other route exists, then source node starts a DSR [11] routing request to search another route. In MANETs, it is possible to find out multiple routes between two nodes.

By routing through an alternative route to the destination node, we check the authenticity of the misbehavior reporter node. When the MRA packet is received by destination through alternative route, the local knowledge base is searched to check whether the reported packet was received or not. If the packet is already received, then

the misbehavior report generated is false and the node is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

By adopting MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

- ***Digital Signature***

EAACK works on an acknowledgment-based IDS. All modules of EAACK (ACK, S-ACK, and MRA) are based on acknowledgment detection schemes. The misbehavior report generation of any node in network is dependent on ACK packets. Thus, to acknowledge that all the packets are untainted and authentic. These three schemes will be vulnerable only if the acknowledgment packets are forged by the attacker.

To address this issue, we integrated digital signature [32] in proposed scheme. The integrity of the IDS, EAACK can be maintained by digitally signing all acknowledgment packets before they are sent out and also verified before accepting the packet. However, we require some extra resources to implement digital signature in MANETs. To solve this issue, we incorporated both DSA [33] and RSA [23] digital signature schemes. To implement digital signature in MANETs we try to find the optimal solution.

5. Performance Evaluation

This section, we will mainly focus on discussing our simulation as well as performance comparison metrics [13] with the help of simulation results among TWOACK, AACK and EAACK schemes.

- ***Simulation parameters:***

We conducted our simulation in the Network Simulator (NS) 2.34 with Ubuntu 16.04 as operating system. The system is running with core i5 and 4-GB RAM.

Table 1: Simulation parameters

channel type	Wireless
MAC type	Mac/802.11
max packet in if q	50
mobile nodes	18
Protocol used for routing	AODV
Topography X dimension	1216
Topography Y dimension	743
simulation end time	50.0

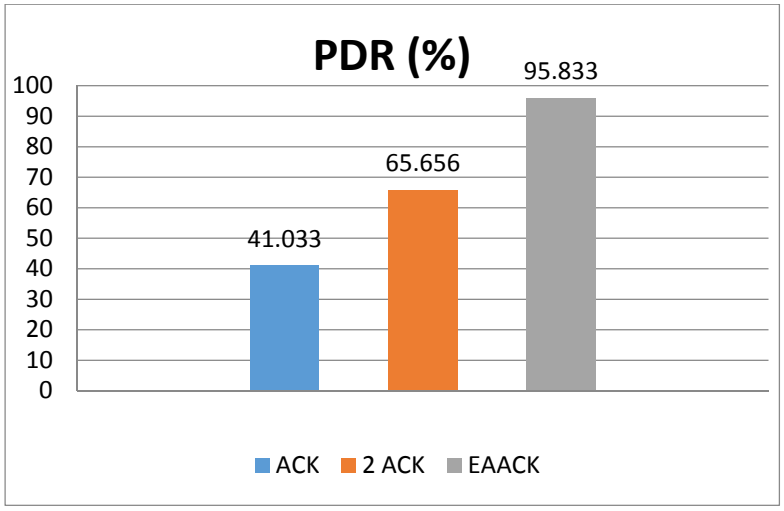
- ***Performance metrics:***

In order to evaluate performance and comparison of our proposed scheme with the existing intrusion detection techniques we adopted three metrices namely: PDR, E2E Delay and Routing overhead and are defined as follows.

Packet delivery ratio (PDR):

The efficiency of network is defined in terms of PDR which in turn shows the efficiency of protocol used for routing. The Packet delivery ratio (PDR) is calculated by following Equation:

$$\text{Packet Delivery Ratio} = \sum \text{Number of packets received} / \sum \text{Total number of packets sent}$$



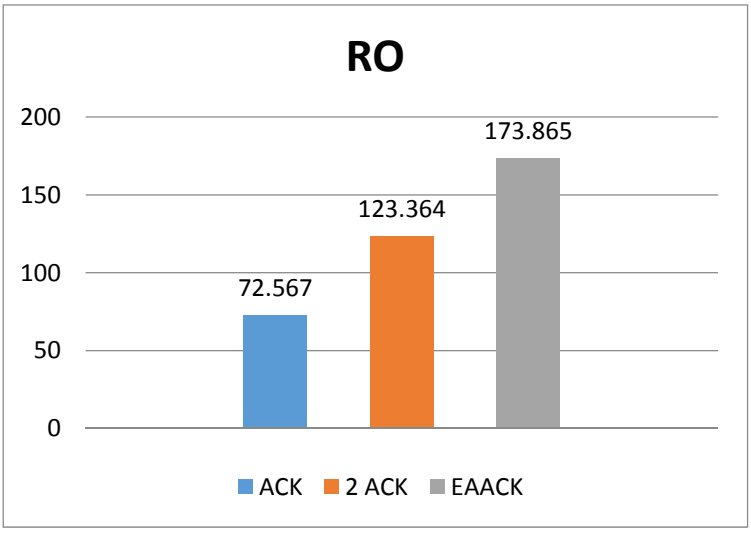
Thus, it gives the ratio of packets that are successfully delivered compared to the number of packets that have been sent out by source. This illustrates the level of delivered data to the destination. Higher the PDR value better is the performance of protocol.

- ***Routing Overhead (OH):***

The routing related transmissions are defined by Routing overhead. It also gives the idea about the resource usage by a specific protocol. The Routing overhead (RO) is calculated by following Equation:

$$RO = \sum \text{Routing transmissions} / (\sum \text{Data transmissions} + \sum \text{Routing transmissions})$$

Thus, it gives the ratio of routing related packets in bytes (RREQ, MRA, RERR, ACK, S-ACK, and RREP) to the total data transmissions and routing in bytes. The lower value of RO means the better performance of the protocol.

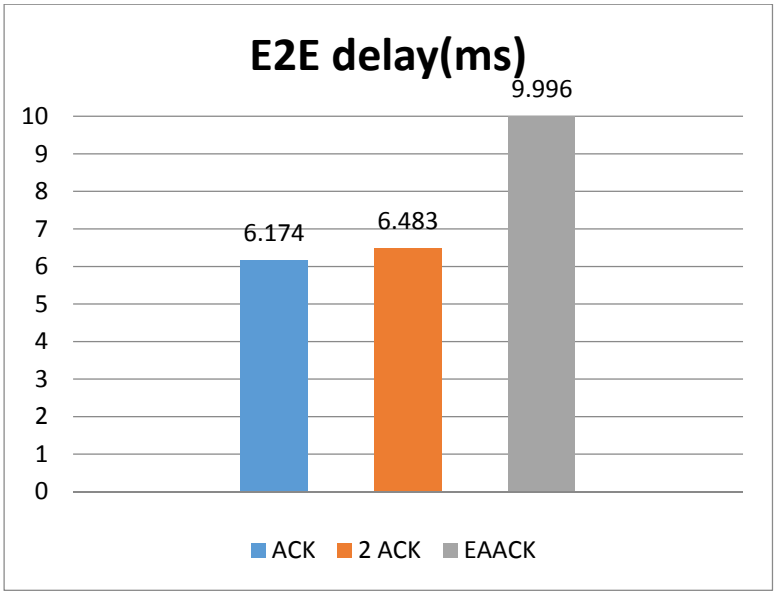


- ***End-to-End delay (E2E delay):***

One of the important design and performance parameter is Network Delay. The delay is nothing but the total time taken by the bit from source to destination.

End-To-End delay = $\sum$ (arrival time – sending time) / $\sum$ Total number of connections

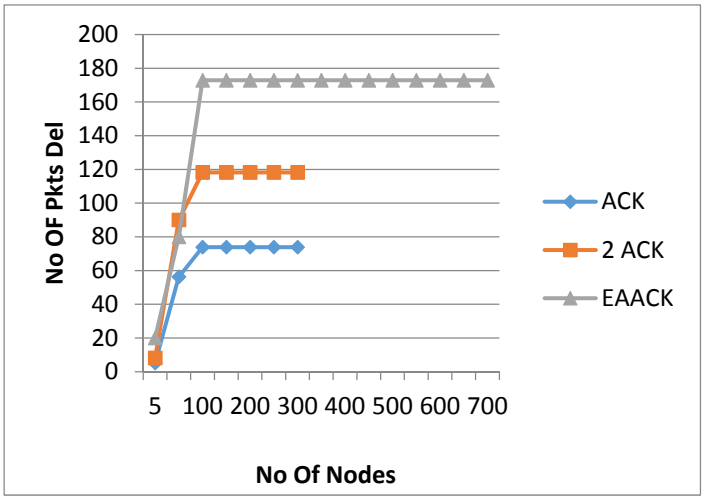
Thus, End-To-End delay is the mean time taken by the packet to reach its destination. This delay includes the queue in data packet transmission and route discovery process. The successful delivery of packet to its destination are only counted. The protocol performs better if it gives lower value of E2E delay.



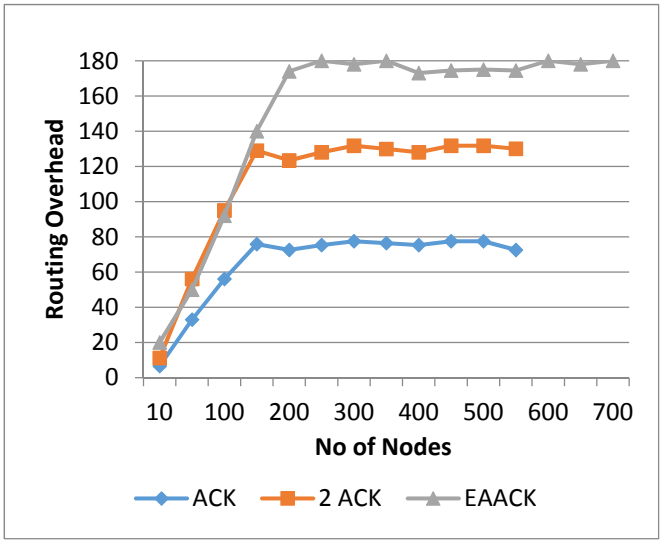
- ***Simulation results (X-GRAPH):***

In this section, the performance analysis of the proposed scheme is done and X-graphs are plotted using these results. Packet delivery ratio, Routing overhead, E2E delay, are the basic parameters used while plotting X-graphs. At last, the comparison is done between EAACK, TWOACK and AACK. Finally, all three results are plotted in graph as shown:

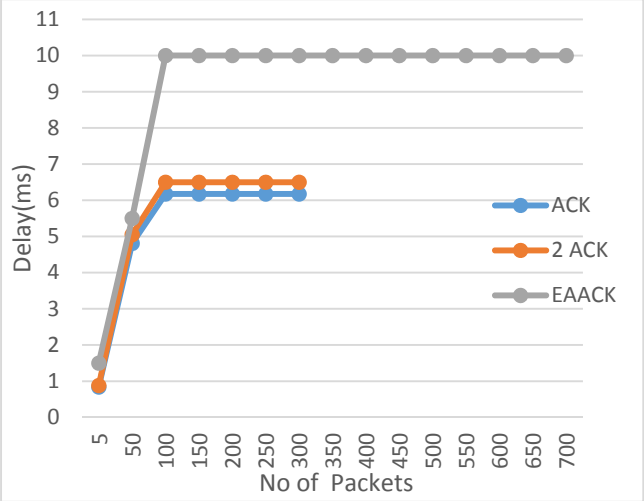
Packet delivery ratio (PDR):



Routing overhead:



End-to-End delay (E2E delay):



6. Conclusion and Future Work

To solve the security issue in MANETS we implemented new IDS based on enhanced adaptive Acknowledgment (EAACK). In this method every acknowledgment packet is digitally signed before sending in network and accepted only after verification. The limited transmission power and false misbehavior of nodes are completely removed in this scheme. Every acknowledgment packet received are authentic and untainted. The given model drastically improves delivery of packets as compared to TWOACK and EAACK. However, the inclusion of digital signature generates more routing overhead. This tradeoff is worthwhile as security of network is more important.

To enhance the merits of EAACK scheme, we will try to research the following issues.

1) Try to implement hybrid cryptography technique to minimize routing overhead due to digital signature.

2) In order to eliminate the predistributed key requirement we will try to examine the possibilities to adopt a key exchange mechanism.

7. References

[1] Y. Zhang, W. Lee, and Y. Huang, \Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[2] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[3] ElhadiM.Shakshuki, Senior Member, IEEE, Nan Kang, and TarekR.Sheltami, Member, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[4] 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.

[5] 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.

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

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

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

[9] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[10]D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5.

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

[12]N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[13]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.

[14]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.

[15]K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbe-haviour in MANETs," IEEE Trans. Mobile Comput.,

[16]S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbe- haviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. MobileComput. Netw., Boston, MA, 2000, pp. 255–265.

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

[18]N. Nasser and Y. Chen, "Enhanced intrusion detection systems for dis- covering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
[19]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.
[20]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.
[21]V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009
[22]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.
[23]J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.
[24]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
[25]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.
[26]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.
[27]K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc net- works on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.
[28]A. Tabesh and L. G. Frechette, "A low-power stand- alone adaptive circuitfor harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[29]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.
[30]B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004
[31]Botan, A Friendly C ++ Crypto Library. http://botan.randombit.net/
[32]Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal In- formation Processing Standards Publication, Gaithersburg MD, 2009, Digital Signature Standard (DSS).
[33]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