IMPROVED EAACK FOR INTRUSION DETECTION SYSTEM

G. Usha Devi[1], Sowmitha MK[2], Jidhesh R[3], Anuradha Jangir[4]

[1]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India*
[2]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India*
[3]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India*
[4]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India*

Abstract

Today Mobile Ad-hoc networks (MANETs) are preferred in many applications because of its self-configuring nature and dynamic topology. Sending node in MANETs rely on intermediate nodes for data transmission to remote nodes. This poses serious security threats. There is a necessity of an intrusion detection system to ensure secure message transmission in MANETs. Many Intrusion Detection Systems (IDS) like Watchdog, TWO ACKnowledgement (TWOACK), Adaptive ACKnowledgement (AACK) and Enhanced Adaptive ACKnowledgement (EAACK) have been proposed for this purpose. Of these IDS, EAACK is found to perform better. EAACK is purely acknowledgement based. Hence there should be a mechanism to validate the acknowledgements. This paper aims at improving performance of EAACK by using hybrid cryptography to validate the sending and receiving nodes in place of Digital Signature Algorithm (DSA) and Rivest Shamir and Adelman algorithm (RSA) that is used in existing EAACK. In hybrid cryptographic key exchange algorithm, a combination of symmetric and asymmetric key cryptographic algorithm (AES and RSA) is used. When compared with its contemporary EAACK, Improved EAACK (IEAACK) achieves smaller network overhead.To simulate the IEAACK environment, NS2 simulator is used. IEAACKovercomes the problems of existing IDS.

Keywords: *IEAACK, IDS, MANETs, TWO-ACK, AACK, AES, RSA, Hybrid Cryptography*

----------***----------

1. INTRODUCTION

Mobile Ad hoc Network (MANET) [1] comprises of nodes that are mobile and has a decentralized infrastructure services. The mobile nodes contain self-configuring and self-maintaining ability. Mobile networks allow data transfer between nodes of different characteristics.Wireless networks, with their low costs and improved technology, have supplanted wired networks.

MANETs are categorized into two for data transmission, single hop and multi hop transmission of data. In a single hop network, the nodes communicate directly with each other within the same radio range frequency.On the other hand, if the nodes depend on intermediate nodes to communicate when it is out of range frequency is known as multi hop data transmission.

MANETs are vulnerable to attacks due to mobility of nodes in open medium and remote distribution of MANETs [12]. For example, malicious attackers can easily capture and compromises nodes and make attack. IDS can be employed to address this issue, as well as enhance the security level of MANETs. IDS usually act as second layer in MANETs and they ensure security in MANETs by working with other existing proactive approaches [4].

2. LITERATURE SURVEY

2.1 Intrusion Detection System in MANETs

Anantvalee *et al.* [3] proposed Intrusion Detection System for MANETs. MANETs always believe in intermediate nodes to transmit data. This gives opportunities for malicious attackers to easily access the data. To overcome this problem, we need a mechanism to provide security. Such a system that identifies attackers in mobile ad-hoc networks and reports them is IDS

Gowthaman et al. [5] discussed four conventional Intrusion Detection Systems in detail. In this section, we describe four existing IDS in detail. They are:

- Watchdog
- TWOACK
- Adaptive Acknowledgement (AACK)
- Enhanced Adaptive Acknowledgement (EAACK)

2.1.1 Watchdog

By this scheme, throughput is improved even in the presence of malicious nodes. The two parts of watchdog scheme are,
1. Watchdog
2. Pathrater

Here, Watchdog acts as IDS that detects malicious behavior of nodes. Watchdog identifies malicious nodes by overhearing the next hop transmission. The failure counter increments, if it comes to know that a node does not deliver packets in predefined time interval. If the failure counter surpasses predefined value, it is marked as malicious nodes. *Pathrater* intimates the routing protocols about the malicious nodes and instructs them to avoid those nodes in routes.

WATCHDOG uses Dynamic source routing protocol and schemeidentifies malicious nodes and not links, so it is very efficient and it is the source of other Intrusion detection

systems in practice. Watchdog fails in the following scenarios
1) Receiver Collisions, 2) Collusion, 3) Ambiguous Collisions, 4) Limited Transmission Power, 5) Partial Dropping and 6) False Misbehavior Report.

2.2.2 TWOACK

TWOACK [13] aims to overcome two failures of watchdog scheme. It solves the problems of limited power supply and receiver collisions. In this scheme, three nodes cooperate with each otherto detect malicious behavior. This is done by acknowledging the data in every two hops it passes.

It works on Dynamic source routing protocol. In figure 1, the working of TWOACK is given. Node A has sent the packet1 to node B and it forwards to C. Since C is two hops away from A, it generates and sends acknowledgement packets to A in the same route.

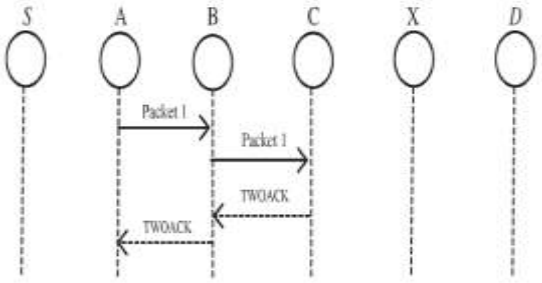

Fig 1 TWOACK scheme: Depicts the working of TWOACK IDS, where acknowledgement is received for every two hops.

If acknowledgement is not received within a predefined time, B and C marked as malicious nodes. This process continues all the way through the route.

TWOACK scheme overcomes two problems of watchdog but, transfer of acknowledgement packets creates considerable amount of overhead. This overhead caused by redundant transmission of acknowledgements becomes a problem in MANETs because of its limited battery power. However, there are many studies going on to preserve energy in MANETs [6].

2.1.3 AACK

Sheltami *et.al* [4], proposed Adaptive acknowledgement (AACK) scheme to reduce the overhead caused because of acknowledgement messages
AACK is a hybrid IDS that combines two schemes

- TACK (similar to TWOACK) and
- ACK scheme (end-to-end acknowledgement scheme)

Firstly, AACK works in end -to- end acknowledgement mode (ACK). The working of ACK mode is given in figure 2. Source transmits the packet to destination node and it is propagated through the route S, A, B, C, X, D and on receiving the packet1, source D generates acknowledgement and sends it to source through the same route in reverse order. This reduces the number of acknowledgement packets that are in transit and hence reduces the overhead imposed. If acknowledgement is received within threshold time, the transmission is successful. Otherwise, it switches to TACK scheme. TACK is identical to TWOACK scheme.

In TACK, three nodes work together to report malicious nodes. This hybrid scheme greatly reduces network overhead but it fails to identify malicious nodes on false misbehavior report and forged acknowledgements.

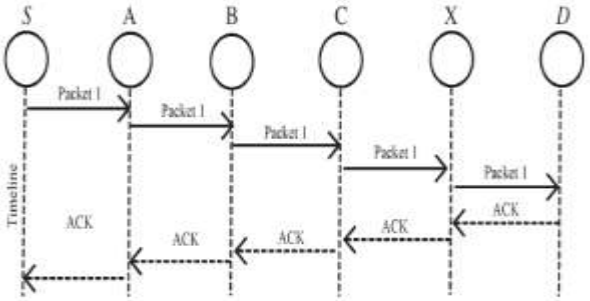

Fig 2 ACK scheme: The destination node sends back acknowledgment packets to source node.

IDS in MANETs like AACK, TWOACK are acknowledgement based and it is crucial to determine the authenticity of acknowledgements. To address this concern schemes were introduced that incorporated digital signature in acknowledgements.

2.1.4 EAACK

The working of EAACK is depicted in the figure 3. This reportedly consists of three schemes namely ACK, SACK and MRA.

This scheme is described in section III as EAACK forms the basis of methodology approached in this paper.

The major part of EAACK is addition of digital signature in acknowledgements to check its validity and authenticity. All the acknowledgements will be signed digitally and sent to the sender of the data. The sender checks for the validity of the recipient using the digital signature.

For, incorporating digital signature, RSA and DSA algorithms have been used separately. This is also a hybrid approach like AACK and overhead imposed by acknowledgement packets is reduced. Here, the number of acknowledgments increases with the increment of malicious nodes. The addition of Digital signature also generates network overhead. It was found that DSA imposes network overhead which is lesser than RSA because of the reduced key size.

However, extensive studies on reducing the network overhead are being done.

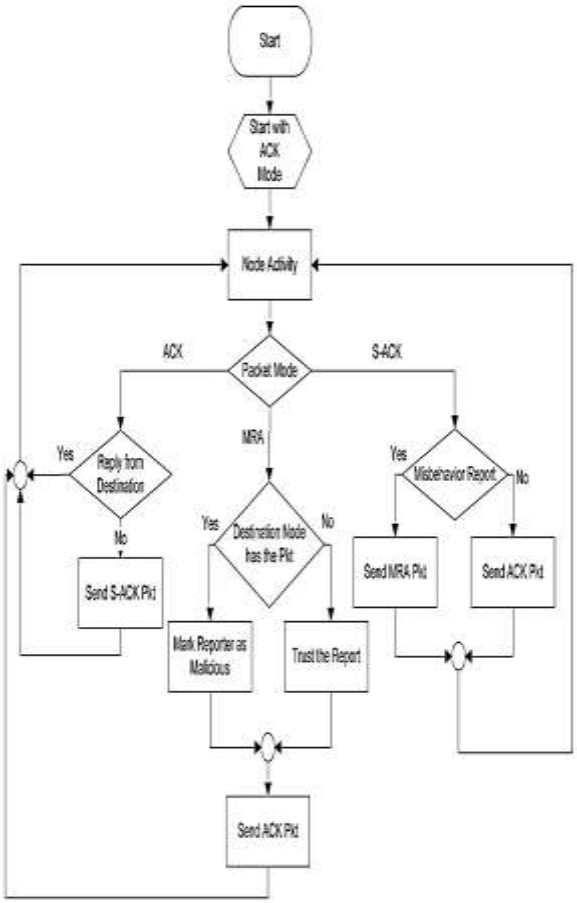

Fig 3 Working of EAACK IDS

2.2 Routing Protocols Used in MANETs

1) Dynamic Source Routing

Daxesh N Patel et al. [7] discussed dynamic source routing scheme for routing in ad hoc networks. The two functions of DSR are: Route Discovery and Route Maintenance.

In Route discovery, route is found by using Route **req**uest (RREQ) and Route **rep**ly (RREP) packets.

In Route Maintenance, link breaks are handled. DSR is a source routing protocol, which is on demand. Each packet contains a route path which consists of the address of nodes which agree to participate in packet routing.

2) AODV

Ashok M. Kanthe *et al.* [8], compares Ad-hoc On-demand Distance Vector (AODV) performance with Dynamic Source Routing (DSR) protocols. The metrics that define performance when comparing AODV with DSR are packet delivery ratio, throughput and delay. It is shown that, performance of AODV surpasses performance of DSR in all of the metrics mentioned even when number of nodes is increased. AODV achieves higher efficiency than DSR in MANETs. AODV is a combination of DSR and DSDV mechanisms. AODV performs the route discovery process more frequent than DSR.

2.3 Cryptographic Algorithms

2.3.1 AES

Sowmya Nag *et al.* [9], discussed various encryption standards. The Advanced Encryption Standard (AES) is based on symmetric encryption scheme. The principle behind AES is "substitution-permutation network", and has fast speed and very low resources consumption. The advantage of AES is that, its computation speed is faster and resource consumption is low. The block size of AES is 128 bits and is fixed and key size can be 128, 192 and 256 bits. AES is very efficient in case of crucial security attacks.

2.4 Digital Signature Algorithms

2.4.1 RSA

Balasubramanian K.,[10] discussed different variants of RSA cryptanalysis techniques. RSA scheme is a method where for digital signatures which uses different keys for encryption and decryption. RSA [14] is a block cipher scheme. The plain and cipher text of RSA scheme are integers between 0 to n-1 for some n. Encryption takes place in blocks. Advantage of RSA is increased security, it provide a method for digital signature. Disadvantage of RSA is that it is very slow in processing and the possible attacks.

3. PROPOSED METHODOLOGY

In this section we describe IEAACK IDS which is based on EAACK IDS. The major modification from EAACK is use of hybrid cryptographic key exchange algorithms for obtaining digital signature. IEAACK uses both RSA and AES (Advanced Encryption Standards) algorithms for validating the acknowledgements. By using Hybrid cryptographic techniques we aim at reducing the network overhead and increase security levels without compromise in the performance.

Working

In the figure 4, there are many nodes, which wish to communicate with each other. IEAACK suspects malicious nodes and reports them.

In IEAACK, we have four parts

- ACK
- SACK
- MRA
- Digital Signature

1. ACK

Once a node sends a packet to the receiver, the packet is propagated through intermediate nodes. When it is received by the destination node, the sender is acknowledged of the receipt in the same route but in reverse order. Within a predefined time (TTL) if the sender does not receive acknowledgements, it switches to S-ACK mode to detect malicious node.

2. SACK

In SACK mode, as the data packets traverse through intermediate nodes, it is acknowledged for every two hops. This will increase number of acknowledgement packets but enhances reliability.

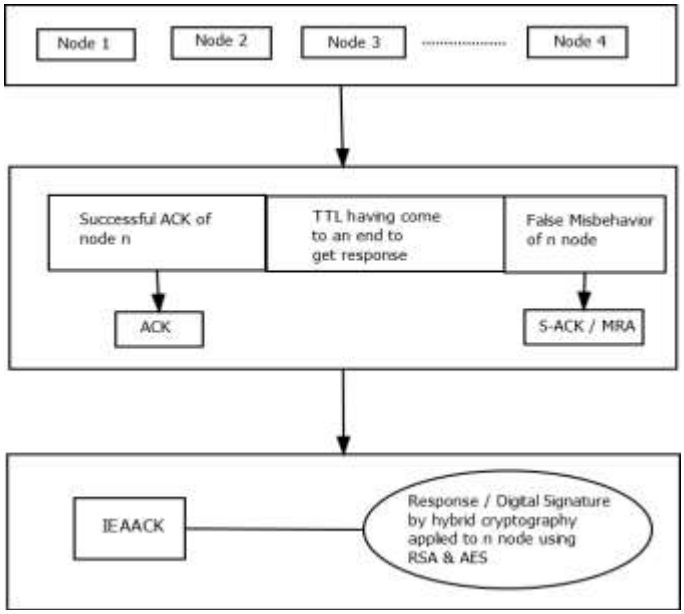

Fig 4. System architecture of IEAACK

In SACK mode, a group of three nodes work together to detect the nodes that are malicious. If a sending node or any intermediate node does not receive acknowledgement within predefined time period, it will tag the next two consecutive nodes as malicious. However, even after successful receipt of acknowledgement, a node may falsely report other nodes as malicious. To overcome this, S-ACK does not believe the misbehavior report immediately but witches to MRA mode.

3. MRA

This scheme aims to identify malicious node in spite of false misbehavior report. Malicious node sends false misbehavior report about other nodes. Here, the source finds an alternate route to reach the destination and send the packet. If the packet is already contained in the receiver's memory, we may say that the misbehavior report was false and the node that sent the false report is malicious.

4. Digital Signature

All the three parts of IEAACK are acknowledgement based. Therefore to validate the acknowledgment, IEAACK uses a combination of RSA and AES algorithm. Hybrid cryptographic techniques generate a smaller key that will reduce routing and network overhead.

3.1 Encryption Techniques

The acknowledgement packets created by destination are digitally signed using RSA digital signature algorithm. The public key of the node is encrypted using AES algorithm and the key generated by AES is shared with the neighboring nodes. The receiver attaches this key and transmits the message to its source through intermediate nodes. This key will be of smaller size compared to the one generated by RSA. Implementing two encryption methods, one for encrypting the plain text (acknowledgement) and the other for encrypting the key will also be a step in increasing the security levels in case of security attacks.

3.2 Decryption Techniques

The source node decrypts the received acknowledgement using public key generated by AES. The obtained plain text is the public key of RSA algorithm and this is used for validating the receiver. If the sender finds out that it is not the actual recipient that has sent the acknowledgement, it sends the packet through alternate route. The packets are retransmitted until message reaches the original destination. This will overcome the forged acknowledgement which was a drawback of Watchdog and TWOACK IDS. By using hybrid techniques, integrity, authentication and confidentiality are ensured.

IEAACK, by using hybrid cryptographic key exchange algorithm reduces the network overhead by reducing the key size used for digital signature and also improves the performance in the cases of forged acknowledgement packets and false misbehavior report when compared with EAACK.

4. SIMULATION ENVIRONMENT

This section describes the simulation methodologies and configurations as well as the various performance parameters which are used for comparing the proposed IEEACK system with the existing systems.

4.1 Simulation Methodologies

In order for comparing IEAACK with the existing systems, the following four scenarios are implemented:

Scenario 1

This scenario is designed to test IDSs performances against false misbehavior report using EAACK. Here a node is set to be malicious to send out false misbehavior report to the source node.

Scenario 2

This scenario is used to test EAACK IDSs performances when the malicious nodes create acknowledgement packets to forge it. At this scenario, a node becomes malicious and sends forge acknowledgment packets to the source node.

Scenario 3

This scenario is designed to test IDSs performances against false misbehavior report using IEAACK with hybrid cryptographic technique. Here, IEAACK uses hybrid cryptography to digitally sign the acknowledgment packets.

Scenario 4

This scenario is used to test IEAACK IDSs performances when forged acknowledgement packets are sent by the malicious nodes with hybrid cryptographic technique.

4.2 Simulation Configuration

The scenarios for comparing IEAACK IDS with other existing IDSs are simulated using NS 2.34. The simulation environment specifies 10 nodes with a size of 400 * 400m. The wireless extension of NS 2 includes both the 802.11 MAC layer and the physical layer. User Datagram Protocol (UDP) traffic with constant bit rate (CBR) with a packet size of 500 bytes and a rate of 0.05Mb is implemented. In this simulation, AODV routing protocol is used for routing and packet forwarding.

4.3 Performance Parameters

Performance of IEAACK is compared with the existing systems using the following performance metrics is used [15]:

1) **Network Overhead:**
Network overhead defines the overall transmission of all types of packets.

2) **Packet Delivery Ratio (PDR):**
It is the ratio of number of packets that are received by the receiver to the number of packets sent by the data origin node. It verifies the packets from source to the destination node.

3) **Average End to End Delay :**
Average End to End Delay measures the time taken by the packets to reach the destination node.

5. RESULTS AND DISCUSSION

The detailed description of the results of the simulation is discussed in this section.

Simulation Results

IDS like Two ACK, AACK, EAACK and IEAACK are all acknowledgement based. The acknowledgement packets generates network overhead. There is a need to reduce this overhead to enhance the performance of the MANETs.

1. Network Overhead

In the figure 5, network overhead of EAACK and IEAACK is compared. Network overhead is considerably reduced in IEAACK when compared with EAACK in the cases of forged acknowledgment packets and false misbehavior report. This is due to the hybrid cryptographic mechanism used in IEAACK.

From figure 5, we can see that network overhead is very high in TWOACK mode and considerably reduced in AACK, EAACK. Network Overhead is further reduced by 18.3% in IEACK in presence of malicious nodes.

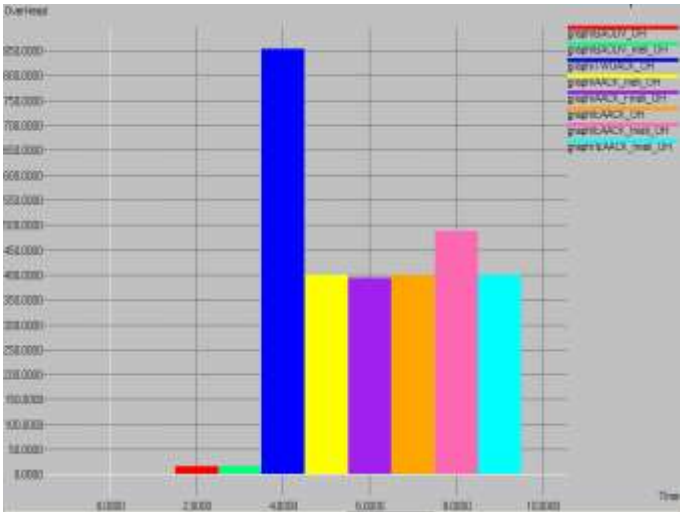

Fig. 5. Comparison of Network overhead in EAACK and IEAACK

2. Packet Delivery Ratio (PDR)

In the figure 6, packet delivery ratio in TWOACK, AACK, EAACK, IEAACK are compared.

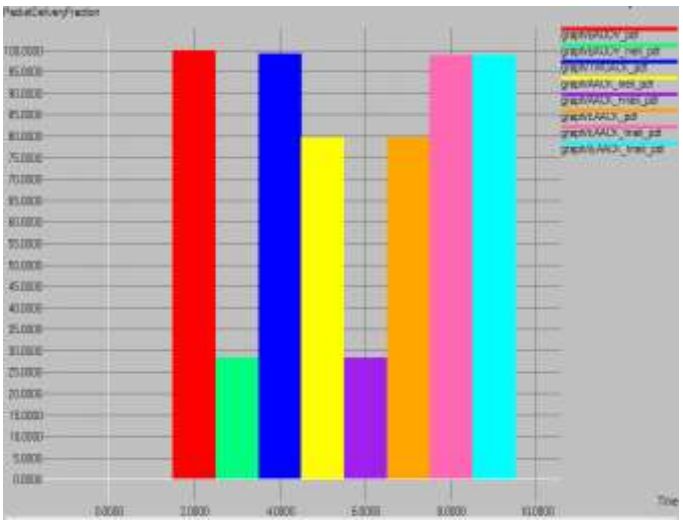

Fig. 6. Comparison of Packet Delivery ratio in EAACK and IEAACK

It is seen that EAACK and IEAACK has a better packet delivery ratio compared to others. This is due to detection of malicious nodes in advance and finding alternate routes for delivery of packets. Packet delivery ratio in IEAACK and EAACK increases by 20% when compared with AACK in the presence of malicious nodes.

3. Average End to End Delay

In the figure 7, a comparison on time taken by a packet to reach destination is made in different scenarios. It has been noted that delay is 18% less in IEAACK and EAACK when compared with AACK.

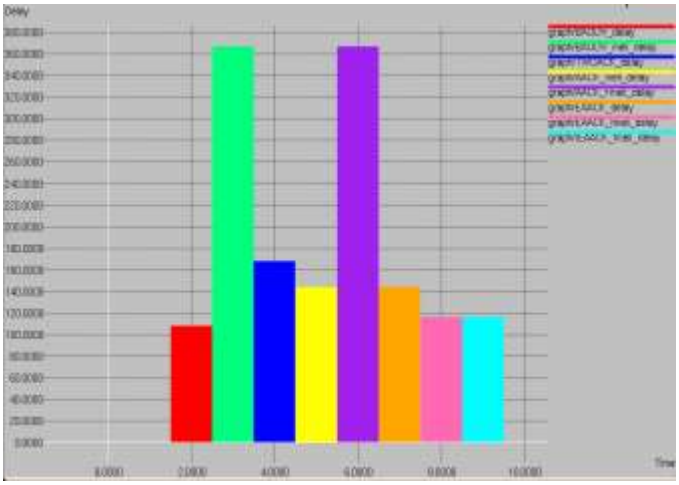

Fig. 7. Comparison of delay in EAACK and IEAACK

6. CONCLUSION

IEAACK has been proposed for MANETs, which is an improvement to EAACK IDS. A model to validate the acknowledgement packets and digitally sign them has been implemented. Adding digital signatures helps us to correctly detect forged acknowledgements. IEAACK also overcomes the security threats posed by false misbehavior report. The results suggest that the proposed scheme reduces the network overhead by 18% without affecting packet delivery ratio and average end to end delay when compared to EAACK IDS.

REFERENCES

[1] Chackho N. M, Sam S and Leelipushpam P. G. J, "A Survey on various privacy and security features adapted in MANETs routing protocol," *in Automation, Computing, Communication, Control and Compressed Sensing*, Kottayam, pp. 508–513, March 2013.

[2] Chadli S, EmharrafM, Saber M, Ziyyat A, "Combination of Hierarchical and Cooperative models of an IDS for MANETs," *in Signal Image Technology and Internet Based Systems tenth IEEE conference*, Marrakech, pp. 230-236, Nov. 2014.

[3] T. Anantvalee and Jie Wu, "Reputation Based System for Encouraging the Cooperation of Nodes in MANETs," *in Communication IEEE international conference*, Glasgow, pp. 3383-3388, 2007.

[4] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A secure Intrusion detection system for MANETs", *IEEE transactions on industrial electronics*, vol. 60, pp. 1089-1098, March 2013.

[5] G. Gowthaman and G. Komarasamy, "A study on Secure IDS in wireless MANETs to increase the performance of EAACK", *in Electrical, Computers and Communication Technologies*, Coimbatore, pp. 1-5, 2015.

[6] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[7] Daxesh N Patel, kothadya S. B, Jethwa P. D, Jhaveri R. H," Asurvey of reactive routing protocols in MANETs", *in Information Communication and Embedded Systems*, pp. 1-6, 2014.

[8] Ashok M. Kanthe, Dina Simunic and Ramjee Prasad, "Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks," *inEmerging Technology Trends in Electronics, Communication and Networking*, 2012.

[9] Sowmya Nag K, Bhuvaneswar H. B, Nuthan A. C, "Implementation of Advanced Encryption Standards-192 bit using multiple keys," *in Research and Technology in the coming decades*, pp. 1-7, 2013.

[10] Balasubramanian K, "Variants of RSA and their cryptanalysis" *in Communication and Network Technology*, pp. 145-149, 2014.

[11] 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, pp. 659-666, 2012.

[12] 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.

[13] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan,"An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Computing.*, vol. 6, no. 5, pp. 536–550, May 2007.

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