Survey on Intrusion Detection Techniques in MANET

[1]Narendra M. Adeshara, [2]Krunal J. Panchal
[1]Master Engineering in Information Technology, [2]Asst. Professor
[1] Gujarat Technological University, Gujarat, India, [2]LJIET, Gujarat, India

***Abstract* - The Mobile Ad Hoc Network (MANET) consists of a collection of wireless mobile nodes. These Mobile nodes are connected by wireless link. This network do not required any infrastructure or centralized access point such as base station. MANETS are highly venerable for Passive and Active Attacks because of their open medium, rapidly changing topology and lack of centralized monitoring. Discussions regarding attacks and intrusion detection techniques on MANET are presented inclusively in this paper, and then the comparison among several intrusion detection techniques is evaluated based on this parameter.**

***Index Terms:* MANET, IDS, IDS Techniques.**

I. INTRODUCTION

Networks are classified into two main types based on connectivity, wired and wireless networks. A wireless network provides flexibility over standard wired networks. Only with the help of wireless networks, the users can retrieve information and get services even when they travel from place to place.

"Ad Hoc" is a Latin word that means "for this purpose". So, we can say that an Ad hoc network is self-configurable network which can operate without any fixed Infrastructure structure. It refers to a network connection established for a single session and does not require or a wireless base stations. It's quick and easy deployment in a situation where it's highly impossible to set up any fixed infrastructure networks, has increased the potential used in different applications in different critical scenarios. Such as battle fields, emergency disaster relief, conference and etc.

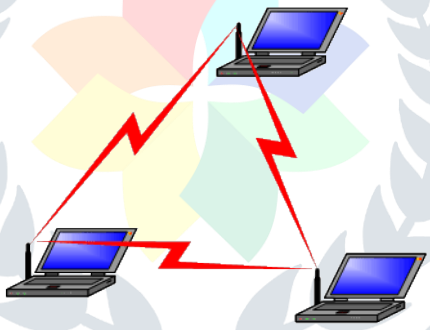

Figure 1 Ad Hoc Network [1]

II. MANET

Mobile Ad hoc Network (MANET) is a group of mobile nodes capable of with mutually a wireless transmitter and a receiver that communicate through each other via bidirectional wireless associates moreover directly or indirectly. The process of configuring MANET could be differing. It depends on application whether it is small or large

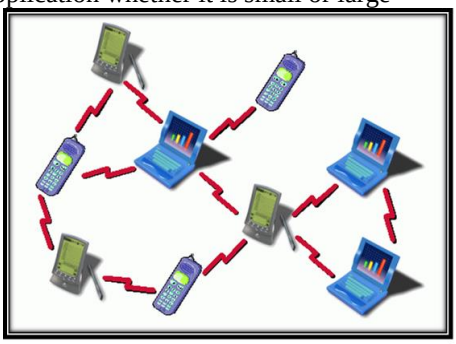

Figure 2 MANET Architecture

Static system is decided powerfully and it is totally controlled with the system which is large scale, mobile and highly active system. Nodes in network work as both transmitter and receiver. Nodes communicate with each other if they are both contained by the same communication range. Or they rely on their neighbors for communication.
One of the most important of wireless networks is it has capability to communication among dissimilar parties, transfer data when they are in mobility. Within the range, this communication between transmitters can be restricted. Two nodes cannot able to communicate outside of the communication range. Intermediate nodes will allow to MANET resolves this complexity.

- There are two kinds of MANETs:
  1) Closed
  2) Open

In a **Closed** MANET, all mobile nodes assist through each other toward a goal, such as emergency search and law enforcement operations.
In an **Open** MANET, various mobile nodes with different goals, share their resources in order to make global connectivity. Resources are consumed rapidly as the nodes participate in the functions. Battery power is measured to be significant in a mobile environment. An individual node of a MANET comprises the benefits of other nodes but it refuses to share its own resources. Such nodes are called as ***misbehaving nodes*** or ***selfish nodes***. A ***selfish node*** may decline to forward the data it received to save its own energy.

- MANET has two types of networks:
  1) Single-hop
  2) Multi-hop

Single-hop network, all nodes communicate directly through each other which are surrounded by the same radio coverage area range. **Multi-hop** network, if the destination node is out of their radio range an individual node should depend on other intermediate nodes to transmit. In MANET, the nodes can easily move and arrange randomly. The wireless topology of the network may be modified rapidly and impulsively. It may control in an unrelated fashion or associated to huge Internet resources. But Attackers can easily insert the malicious or incorporate nodes in the network to attain attacks [8].

III. ROUTING PROTOCOL FOR AD HOC NETWORK

In mobile ad hoc networks, due to the limited wireless transmission range, it is usually the case that paths between source nodes and destination nodes require multiple hops. So, every node may act as a router to forward packets. Also, due to the nodes mobility, it is necessary to change the existing routes in order to maintain the connection between them. MANET routing protocol must be able to quickly detect and respond to such state changes in order to minimize degradation in services provided to existing sessions.

- In general, routing protocols can be classified into two main groups: **Proactive routing** and **Reactive routing**.

Proactive routing constantly formulates routing choices in order to have accessible paths available for nodes that need to send packets [3]. **Reactive routing** on the other hand only finds a route when requested; as soon as a node has a packet to transmit, it queries the network for a route.

IV. ATTACKS ON MANET [10]

Network layer attacks in MANETs can be divided into two main categories, namely **Passive attacks** and **Active attacks**.

1) Passive Attacks:

Attacker does not disturb the operation of the routing protocol but attempts to see some valuable information through traffic analysis. This can be lead to the disclosure of critical information about the network or nodes such as the network topology.

A. Eavesdropping

The unintended receiver could read the original message and could inject fake message to the network.

B. Traffic Analysis and Location Disclosure

It identifies the communication parties and functionalities.

2) Active Attacks

Intruders launch malicious activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network.

A. Routing Attacks

1. **Routing Table Overflow:** The goal of this attack is to overflow the target systems routing table and to prevent of new routing table entries to authorized nodes by creating routes create to non-existed nodes by the attackers.

2. **Routing table poising attack:** The compromising nodes sends fictitious routing updates/modify route update packets sent to other authorized nodes. It results in congestion in a portion of network or makes that part inaccessible.
3. **Routing cache poising**: In reactive routing protocols each node maintains a route cache. This attack occurs when information to be stored is deleted or altered with false information in cache. It has same objectives as same as routing table poising attack**.**
4. **Rushing Attack**: This attack is mostly difficult to detect. An attacker on receiving RREQ packet quickly floods the packet throughout the network before other node can react who receive the same RREQ.
5. **Packet Replication**: Attacker replicate packets which consume additional bandwidth and battery power resource**.**

B. Black Hole Attack

The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out by the destination node.

C. Grey Hole Attack

In which an intruder first captures the routes, and then drops packets selectively. BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason.

V. IDS

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions.

The development of IDS is motivated by the following factors:

- Existing systems have security was that render them susceptible to intrusions, and finding and fixing all these deficiencies are not feasible.
- It is almost impossible to have a fully secure system.
- Even some secure systems are vulnerable to insider attacks.

Intrusion detection system is used to detect many types of malicious behaviors of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET knows how to detect the attackers as soon as they enter the network, we will be able to completely remove the potential damages caused by compromised nodes at the first time. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. The present research mechanism has focused on designing Intrusion Detection Systems (IDS) to monitor and analyze system events for detecting network resource misuse in a MANET.

VI. ISSUES IN INTRUSION DETECTION SYSTEM

MANET's dynamic topology makes conventional IDSs ineffective and inefficient for this new environment. There are some new issues which should be taken into account when a new ID is being designed for MANETs.

- **Lack of central points**: MANETs do not have any entry points such as routers, gateways, etc. present in wired network. A node in a MANET can see only a portion of a network: the packets it sends or receives together with other packets within its radio range.
- **Mobility**: MANET nodes can leave and join the network and move independently at any time, so the network topology can change frequently and cause traditional techniques of IDS to be unreliable by its highly dynamic operation.
- **Limited Resources**: Mobile nodes generally use battery power and having different capacities. The computational and storage capacities also varied. The variety of nodes, with scarce resources, affects effectiveness and efficiency of the IDS agents they support.

VII. IDS IN MANET

As discussed before, Nodes of MANETs assume that other nodes always cooperate with each other to relay data. This assumption makes the attackers with the opportunities to achieve significant impact on the network with just one or more compromised nodes. To solve this problem, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we can completely eliminate the potential damages caused by compromised nodes at first time. IDSs act as the second layer in MANETs. In this particular section, we describe three existing approaches namely, Watchdog, ExWatchdog, TWOACK, 2ACK, AACK, EAACK and A3ACK.

A. Watchdog [2]

(S. Marti, T. J. Giuli, K. Lai, and M. Baker) Watchdog that aims to improve throughput of net-work with the presence of malicious nodes. Actually, the watchdog scheme is consisting of two parts, called Watchdog and Path rather. Watchdog works as an intrusion detection system in MANETs. It is to detect the malicious nodes which are misbehaving in the network. Watchdog detects malicious node by promiscuously listens to its next hop's transmission. If Watchdog node detects that its next node fails to

for-ward the packet within a certain period of time, it in-creases its failure counter. In Watchdog, whenever a node's failure counter exceeds a predefined threshold, the node reports it as misbehaving. In future transmission, the Pathrather cooperates with the routing protocols to avoid the reported nodes. Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many IDSs for MANET are either based on or developed as an improvement to the Watchdog scheme.

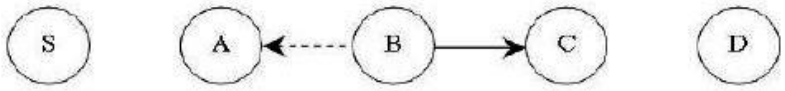

Figure 3 Watchdog Operation [2]

B. ExWatchdog [3]

Nasser and Chen (Kachirski O, Guha R, 2003) have proposed techniques to identify IDS called ExWatchdog that is actually an extension of Watchdog. ExWatchdog also detects intrusion from malicious nodes and reports this data to the response system, i.e., Pathrater or Routguard. Watchdog which is based on overhearing resides in each node. Each node can detect the malicious action of its neighbors through overhearing and can report this misbehaving to other nodes. However, if the node that is overhearing and reporting is malicious itself, it can make a serious impact on network performance. The main feature of the proposed system is the ability to detect malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then it proceeds to protect the network. So, ExWatchdog solves the fatal problem of Watchdog.

C. TWOACK [4]

TWOACK scheme proposed by (Kashyap Balakrishnan, Jing Deng and Pramod K. Varshney). TWOACK is neither an enhancement nor a Watch-dog based scheme. Aiming to improve the performance of Watchdog, TWOACK acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination to detect misbehaving links. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required routing protocols such as Dynamic Source Routing (DSR) to work on. The working process of TWOACK is, 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,it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains route from node A to node C ,which is called reverse route and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. If this TWOACK packet is not received in a predefined time period, both nodes B and C are re-ported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added un-wanted network overhead. Due to the limited battery power nature of MANETs, redundant transmission process can easily degrade the life span of the entire network.

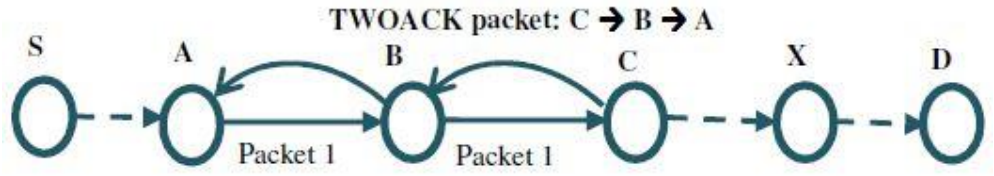

Figure 4 TWOACK Scheme [4]

D. 2ACK [5]

The 2ACK scheme proposed by (K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan) is a network layer technique to detect misbehaving links. The 2ACK scheme detects misbehavior through using acknowledgment packet namely 2ACK. This packet is sent by a node to two nodes down the line along the route. From the figure it can be seen that N1, N2, and N3 are three consecutive nodes along the transmission path. The routing protocol DSR determines the route from source node S to destination node D in the Route Discovery Phase. N1 sends data packet to N2 and then N2 sends the data packet to N3, but N1 cannot ensure whether N3 receives the data packet or not. This happen seven when no nodes in the path are misbehaving nodes. This problem becomes severe when the nodes misbehave in MANETs. Hence to overcome this problem the 2ACK scheme ensures that each node sends an acknowledgement packet two hops down the line along the route in opposite direction i.e. Node N3 on successful reception of data packet must send the acknowledgement 2ACK to N1 via N2. This acknowledgment 2ACK contains ID of the corresponding data packet received by N3. This 2ACK transmission takes place for every set of three nodes. Therefore, only the first node next to source will not send the 2ACK packet and only the last node just before destination & destination node both will not receive the 2ACK packets. Each node in the transmission path maintains the list of IDs of packets that are sent from it for a predefined time say T seconds. If the 2ACK is received within T seconds, then the ID of that packet which is received successfully

by third node (node that sends acknowledgement) will be deleted from list at the node receiving 2ACK. Otherwise the ID is deleted from the list after T seconds and failure count will be incremented.

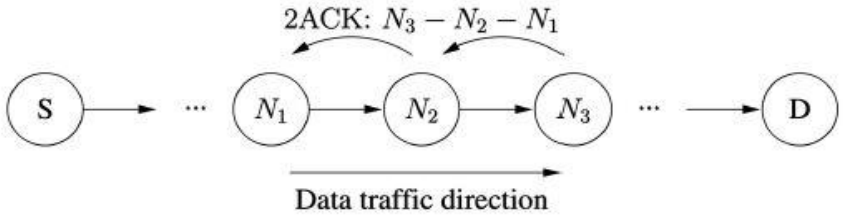

Figure 5 2ACK Scheme [5]

E. AACK [6]

AACK scheme proposed by (Tarek Sheltami, Anas Al-Roubiney,Elhadi Shakshuki and Ashraf Mahomoud). It is based on TWOACK Acknowledgement (AACK), AACK is an acknowledgement- based network layer scheme which can be considered as a combination of a scheme call ACK (identical toTWOACK) and an end-to-end acknowledgement scheme called ACK. When compared to TWOACK, AACK reduce the network overhead while still capable of maintaining or even surpassing the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The network overhead is greatly reduced by this hybrid scheme in AACK, 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. Many of the existing IDSs in MANETs adopt acknowledgement based scheme, TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is necessary to guarantee the acknowledgement packets are valid authentic.

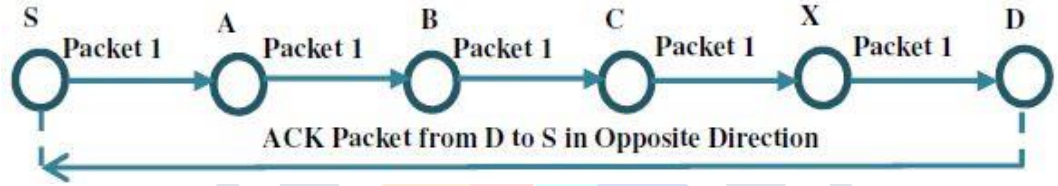

Figure 6 AACK model of AACK Scheme [6]

F. EAACK [7]

EAACK scheme proposed by (N. Kang, E. Shakshuki, and T. Sheltami). The Advancement of AACK with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).Here ACK acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. The S-ACK scheme which is an improved version of the TWOACK lets every three consecutive nodes work in a group to detect misbehaving nodes. For every 3 consecutive nodes in the route, the third node is required to send an S-ACK packet to the first node. The motive of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. Unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, the EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a certain step to detect false misbehavior report [7].

G.A3ACK [8]

A3ACK scheme proposed by (Tarek Sheltami, Elhadi Shakshuki and Abdulsalam BAsabaa). Adaptive Three Acknowledgements (A3ACKs) scheme is an extension of the AACK scheme. It aims to solve three weaknesses of the Watchdog scheme, which are limited transmission power, receiver collision and collaborative attacks/collusion attack especially if there are two consecutive collaborative misbehaving nodes in a route path. In this scheme we assume that the misbehaving nodes cooperative to forward routing packet but they drop data packets. The A3ACKs technique is an acknowledgement-based scheme based on Dynamic Source Routing Protocol (DSR). It consists of three main models named, End-To-End Acknowledgement (AACK) model, Two Acknowledgement (TACK) model and Three Acknowledgment (THACK) model. The data packet in each model is different according to flag indicator as shown in Table 1, where we use only 2 bit of DSR reserved header in order to classify packet types for each model. In the A3ACK, the default model is AACK model which is similar to AACK mode in AACK scheme [6] as shown in figure 2.4, where the source node S first sends data packet to destination node D along the active route that is gets from DSR routing protocol. Also, the source node S has to register the sending packet ID and sending time. When destination D receives the sending data packet, it has to generate an AACK packet and sends it back to the source node on the same route path but in opposite direction. If the source node S didn't receive the AACK packet with predefined timeout, it has to switch to Tack model to detect if there is any misbehaving nodes in active route path. The TACK model works similar to TWOACK scheme, except that it detects misbehaving nodes instead of links. In Tack model, the third node for every three consecutive nodes in route path has to send back a Tack packet to first node. This process carries out by every three consecutive nodes in a route path as

shown in figure 2.5. If the source node S fails to receive acknowledgement packet (TACK) within a predefined timeout, it has to switch to THACK model to detect if there are any collaborative misbehaving nodes in the route path. The THACK model aims to solve the problems of receiver collision and limited transmission power and collaborative attacks as well within presence of two consecutive misbehaving nodes in a route path. In the THACK model, every four consecutive nodes in path work together where the fourth node (three hops away from the first one) has to send back an THACK packet to the first node in that group within a predefined time out.

Table 1 Packet Type Indicator for A3ACK Scheme

Packet Type	AACK	TACK	THACK
Packet Flag	01	10	11

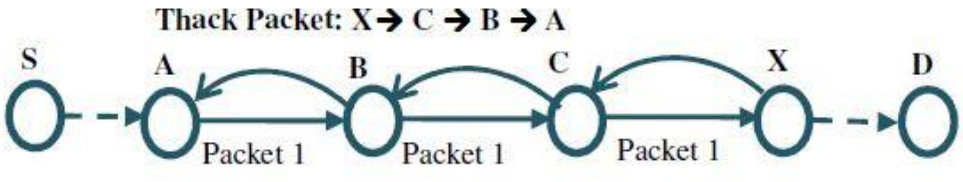

Figure 7 A3ACK Scheme [8]

VIII. CONCLUSION

This paper summaries basics of MANET, challenges and attacks in and briefly describes different Intrusion Detection Techniques in MANET and also provides comparison between them (Refer Appendix A). Intrusion-Detection Systems aims at detecting attacks and malicious nodes against computer systems and networks; in general, attacks against information systems .IDS Techniques can be viewed as a guard system that automatically detects malicious activities within network also improve network performance.

APPENDIX

APPENDIX A: COMPARISON BETWEEN IDS TECHNIQUES

	TITLE	AUTHOR	METHODS	ADVANTAGES	DISADVANTAGES	ROUTING PROTOCOL
1	Mitigating routing misbehavior in mobile ad hoc networks	S. Marti, T. J. Giuli, K. Lai, and M. Baker	Watchdog and Pathrater	Increase the throughput.	Increasing the overhead transmissions.	-
2	TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks	Kashyap Balakrishnan, Jing Deng and Pramod K. Varshney	TWOACK	Detect Selfish node and overall end-to-end PDR improve.	Routing Overhead	DSR
3	Enhanced intrusion detection systems for discovering malicious nodes in mobile adhoc network	N. Nasser and Y. Chen	ExWatchdog	Decrease the overhead greatly, solves a fatal problem	Does not increase the throughput, falsely report	-
4	An acknowledgment-based approach for the detection of routing misbehavior in MANETs	K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan	2ACK scheme	Reduce extra routing overhead, does not suffer from transmission power problem.	Computational complexity and time complexity of the system is high.	DSR

5	Video Transmission enhancement in presence of misbehaving nodes in MANET	Tarek Sheltami, Anas Al-Roubiney,Elhadi Shakshuki and Ashraf Mahomoud	AACK (Adaptive Acknowledgement)	Better routing packet delivery and better PDR compare to TWOACK	Significant delay in End to end Ack	DSR
6	Detecting misbehaving nodes in MANETs	N. Kang, E. Shakshuki, and T. Sheltami	EAACK (Enhanced Adaptive Acknowledgement)	Higher malicious behavior detection rates, positive performances in various test scenarios	It suffers from extra amount of network overhead	DSR
7	Implementation of A3ACKs IDS under various mobility Speed	Tarek Sheltami, Elhadi Shakshuki and Abdulsalam BAsabaa	A3ACK (Adaptive Three Acknowledgements)	Improved network performance with or without presence of consecutive collaborative misbehaving nodes.	Routing overhead increased.	DSR

REFERENCES

[1] http://www.identi.li/index.php?topic=37655

[2] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, in 6th International Conference on Mobile computing and Networking, MOBICOM'00, P255-265, Aug 2000.

[3] Nidal Nasser. And Yunfeng Chen, 'Enhanced Intrusion Detection System for Discovering Malicious nodes in Mobile Ad hoc Networks', Proceeding of 7th International Conference on Communication, 2001, pp. 1154-1159.

[4] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[5] Liu, K., Deng, J., Varshney, P. K., and Balakrishnan, K. 2007. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. IEEE Transactions on Mobile Computing 6, 5 (May. 2007), 536-550. DOI= http://dx.doi.org/10.1109/TMC.2007.1036

[6] Sheltami, T., Al-Roubaiey, A., Shakshuki, E. and Mahmoud, A. 2009. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282.

[7] 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.

[8] A. Basabaaa, T. Sheltamia and E. Shakshukib "Implementation of A3ACKs intrusion detection system under various mobility speeds" in 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014),ScienceDirect, pp. 571-578.

[9] Shakshuki, E., Kang, N., Sheltami, T., "EAACK – A Secure Intrusion Detection System for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no., pp. 1089-1098, 2013.

[10] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.