Cluster Based Enhanced Adaptive Acknowledgement Technique in Manets for Intrusion Detection

K . Naveen
M.Tech (Cse)
Site, Tirupati

A . Chakradhar
M.Tech (Cse)
Ascet, Gudur

S . Ramaiah
Asst.Professor,
Kmmits,Tirupati

***Abstract*:- Mobile Adhoc Network (MANET) is collection of wireless mobile nodes that are free to in any directions at any speed. Mobile nodes are equipped with a wireless transmitter and a receiver that communicate directly with each other or forward message through other nodes. The MANETs can provide openness and scalability for all the mobile users. Due to this openness and lack of physical protection of MANETs, the attackers can easily attack on network. To develop efficient intrusion detection system (IDS) for mobile Adhoc networks is crucial task. The different intrusion detection systems can propose solutions for different problems. In this paper we can propose an intrusion detection system named as Cluster based enhanced adaptive acknowledgement technique which can find the malicious and misbehaving nodes in the network and also it can reduce network overhead caused by acknowledgement packets hence it will give more throughput and increases packet delivery ratio.**

Keywords:-Mobile Adhoc Network, Intrusion Detection System, Misbehavior of nodes, Acknowledgements, Cluster based routing.

I. INTRODUCTION

An ad hoc network is a collection of mobile devices that can dynamically move and can reorganize themselves and communicate over wireless links. These mobile devices are also autonomous nodes, which serve as routers that forward packets onto the next link. There is no centralized or central server that organizes routing of these packets. Routing to the destination is established at the nodes, which needs to be determined before or after the reception of packets. An ad hoc network consists of mobile platforms known as nodes, 'which are free to move around arbitrarily [9], [23]. These nodes, which are very small, may be located in buildings, trucks, and cars or maybe on a battlefield. MANET is capable of creating a self-configuring and self-maintaining network without any help of a centralized configuration of network, which is widely used in different applications like military conflict or disasters recovery. Low configuration and fast deployment make MANET ready to be used in emergency situations where an infrastructure is unavailable or unfeasible to install in scenarios like natural disasters [16].

The open medium and remote distribution of MANET make it easy to various types of attacks. For example, due to the lack of physical protection for nodes, the attackers can easily compromise nodes to achieve attacks. By considering that most of the routing protocols in mobile Adhoc networks that every node in the network behaves cooperatively with other nodes and may be not malicious [4]; attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. In such it is crucial to develop an intrusion-detection system (IDS) for MANETs [1], [13]. The different characteristics of MANETs lead to different problems. The limited power of mobile nodes leads to limited transmission problems. The transfer data between nodes without knowledge of other nodes leads to collision problems. The malicious attackers can easily compromise nodes and performs misbehavior through the network. Active attack disturbs the normal operation of network by altering it. Packet Dropping Attack is an Active attack, which intentionally drops the packet. There are many reasons for packet dropping intended and un- intended misbehavior. Here we are considering the intended misbehavior is malicious behavior. The main purpose of malicious node is to disrupt the network and affect its availability. All these problems can be overcome by using different IDS systems

In this study we proposed a mechanism, Cluster Based Enhanced Adaptive Acknowledgement technique which can eliminate the intrusions and misbehavior of nodes before establishing of route between source and destination. The false misbehavior report and detection of malicious nodes are having solution with this new IDS mechanism.

In this paper next we are going to be discuss the detailed study of previous IDS systems in section II, The proposed new IDS technique can seen in section III, the section IV can give the simulation results between previous IDS and the proposed one, Finally I will Conclude and suggest future work of paper in section V.

II. THE INTRUSION DETECTION SYSTEMS FOR MANETS

As we discuss before that the mobile Adhoc network is vulnerable for attackers. The nodes in MANET are easily co-operated with other nodes due to their openness and scalability. The attackers can easily compromise the nodes and leads to disturb the network. In MANET, intrusion detection and response systems should be both distributed and cooperative in order to fulfill the needs of mobile ad hoc networks, every node in the mobile ad hoc network participates in intrusion detection and response. Since every node can trust its neighboring nodes, it is responsible for identifying the signs of intrusions locally and uniquely. However, neighboring nodes can interactively exchange messages in case of a suspicious detection or confirmed intrusion identification. The attacker can perform Black Hole Attack [18] against the routing by a malicious node itself it can advertise as shortest path through the nodes and it was intercepted, whose packets it will want. The different IDS systems can have the solution for all these problems.

Watchdog Mechanism

The watchdog method, as implemented by Marti, Giuli et al in [15], detects misbehaving nodes acting alone by maintaining a buffer that contains recently sent packets. In the watchdog mechanism the watchdog can be placed in every node on the network. Watchdog can be implemented on DSR [10] protocol. When a node forwards a packet, the node's watchdog confirmed that the next node in the path also forwards the packet. The watchdog does this by listening to the next node transfer of data. If the packet does not forwarded by next node then it is called as misbehaving of node.

In other words, in this scheme, every packet that is overheard by the watchdog is compared with the packet in the buffer to see if there is any matched packet. If any match will find in the buffer then the packet has been successfully delivered and it is removed from the buffer. If a packet has remained in the buffer beyond the timeout period then a failure counter for the node responsible for forwarding the packet is incremented. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving node. In this case, the Pathrater will give information to the other nodes with the routing protocols to avoid the reported nodes in future transfer of packets. The pathrater can divide the malicious or misbehavior node from the network by sending the malicious node address to every node in the network.

Watchdog scheme can identify the malicious nodes and cannot identify the malicious links. Watchdog scheme will fail to detect 1.Reciver collisions 2.Ambiguous collisions 3.Limited transmission power problems 4.False misbehavior report 5.Collusion 6.Partial dropping. Due to these problems we shall move to another technique to overcome some of these problems.

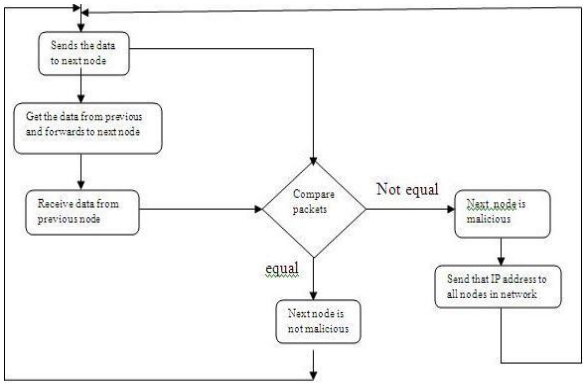

Fig: 1. Watchdog scheme at every node in the network

TWOACK Mechanism

Some of the problems of watchdog scheme can be solved in this technique. This scheme can be designed to solve the receiver collisions and limited transmission power problems of watchdog scheme. The TWOACK [14] is a network-layer technique to detect misbehaving links. It can be implemented on dynamic source routing protocol. The TWOACK technique detects misbehavior through the use of a new type of acknowledgment packet, termed TWOACK. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route.

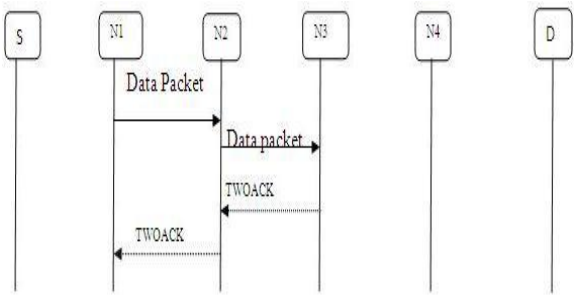

Fig: 2. TWOACK scheme: Every third node in group of three nodes sends ack to first node

The operation of the TWOACK is that N1, N2, and N3 are three consecutive nodes along a route. The route from a source node to a destination node is identified by using DSR protocol. When node N1 sends a data packet to next node and it forwards to next node N3, it is unavailable to N1 whether N3 receives the data packet successfully or not. Such an uncertainty exists even when there are no misbehaving nodes. The problem becomes

much more serious in MANETs with potential misbehaving nodes.

The TWOACK mechanism requires an explicit acknowledgment to be sent by N3 to notify N1 of its successful reception of a data packet: When node N3 receives the data packet successfully, it sends out a TWOACK packet over two nodes to N1 (i.e., the opposite direction of the actual routing), with the ID of the current transfer data packet. Such a TWOACK transmission takes place for every set of three nodes along the route. Therefore, only the first node from the source will not act as a TWOACK packet sender. The last node before the destination and the destination node will not serve as 2ACK receivers.

The problems with this technique are, the no of acknowledgement packets can be increased more and more that leads to increase in the network overhead and due to the low battery resources the life span of the network will be decreased.

Adaptive Acknowledgement (AACK) Mechanism

Adaptive acknowledge scheme is also based upon the acknowledgement packets. By using AACK [21] technique the network overhead caused by acknowledgement packets in the above technique is to be reduced. The AACK is the combination of two systems they are End to End Acknowledgement system and Enhanced TWOACK (TACK) system.

An End to End scheme can send the data packets from source to the destination by using the Adhoc On Demand Distance Vector Routing algorithm (AODV). After successful receiving of data packet the destination will send the Acknowledgment packet in the same route in reverse direction. If the ack packet is reached to source then the data transfer is successful otherwise it changed to TACK mode to finding the malicious nodes in the route.

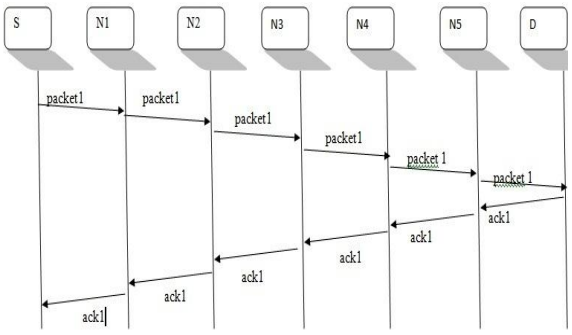

Fig: 3. End-to-End Acknowledgement scheme in AACK Mechanism

The AACK can change to TACK technique for finding the malicious nodes. By examine the transferring route of data packet it can identify the malfunctioning node or attacker. The AACK is still suffering to find false misbehavior report of nodes.

ENHANCED ADAPTIVE ACKNOWLEDGEMENT TECHNIQUE:

In this technique [20] it can give the solutions for the watchdog mechanism failures. These IDS can provide the solutions for problems like false misbehavior report, limited transmission power problems, receiver collisions and detecting malicious nodes.

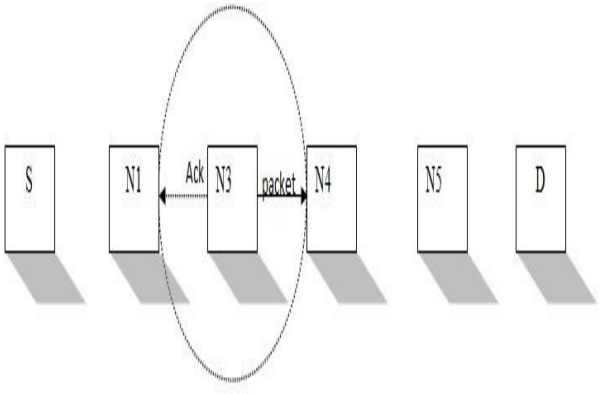

Fig: 4. Limited Transmission power of node N3, it is unable to send data to N5

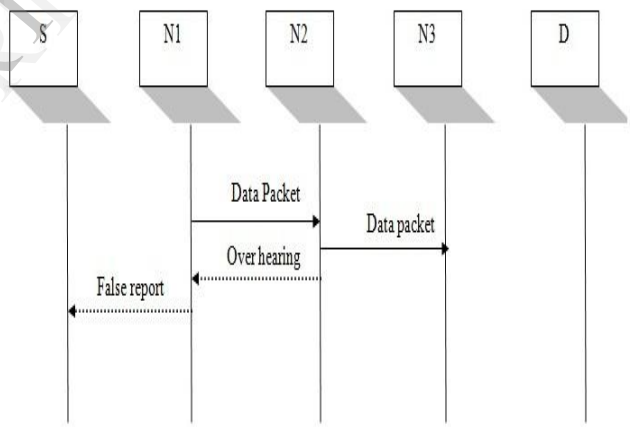

Fig: 5. False Misbehavior report, Node N1 sends false report to source even if node N2 sends packet to node N3

EAACK IDS Description:

This technique will adding additional feature for the previous technique, when there is malicious node find in the previous techniques it check whether the misbehavior report is right or not. This IDS is a combination of three techniques namely End to End Acknowledgement technique, Secure Acknowledgement technique and Finding Misbehavior report. To distinguish the different techniques by using different packet types we can use 2-bit header for describing the type of packet it can send.

PACKET TYPE	2-BIT INDICATIION
Normal Data Packet	00
End-to-End Acknowledgement	01
Secure Acknowledgement	10
Finding Misbehavior Report	11

Table: 1. Indicating packet type through 2-bit header in EAACK technique

End-to-End ACK:

It is same as previous end to end acknowledgement scheme in AACK, but it act as part of the hybrid scheme in this IDS System. The main aim of using this scheme is to reduce network overhead caused by acknowledgement packets. The data can transfer from source to destination by using AODV protocol which leads to detect the route between nodes, after reaching the data to the destination the destination will send back an acknowledgement package to the source via the same route in reverse direction. If the acknowledgement cannot reach the source with predefined time, then it sends the Secure Acknowledgment packet to detect malicious nodes.

Secure ACK:

This Secure Acknowledgement technique is the enhanced version for the TWOACK scheme. The main aim of this technique is to identify the malicious nodes in the group for every three nodes. When the data reached to third node in the group then it sends Secure Ack packet to the first node of the group, when the Secure Ack packet does not reach to first node then it sends the information to the source the second and third node of the group are malicious. To identify and confirming of these nodes are malicious the IDS can switch the source to Finding Misbehavior report mode.

Finding the Misbehavior Report:

This technique can be designed to find whether the misbehavior report is right or wrong. The source node can initiate this technique and search the its local knowledge for finding of the other alternative route to reach the destination, if it is not available then it initiates DSR routing protocol to find the alternate route to reach the destination. After reaching this packet to destination it will searches and compare the reported packet is present or not. If it is received it will conclude that the malicious report is wrong and who reported as malicious is malicious node, otherwise the malicious report is right.

This IDS is acknowledgement based technique, all three methods can use the acknowledge packets. The network overhead will be increase more and more due to this large number of acknowledgement packets. For this reason we can propose a new hybrid routing and intrusion detection system to overcome these problems.

III. CLUSTER BASED ENHANCED ADAPTIVE ACKNOWLEDGEMENT TECHNIQUE:

The cluster based enhanced adaptive acknowledgement (CEEACK) technique is used to reduce the network overhead and detecting the malicious nodes in the network. It can uses cluster based routing protocol and enhanced adaptive acknowledgement technique.

Cluster based routing protocol:

The CBR protocol obtains efficient communication and also provides scalability in large mobile Adhoc networks by using clustering technique. The clustering algorithm can divide the nodes as clusters or subnets by the affinity of geography, motion, or task. The affinity is defined by using some similarities between nodes such as group motion or activities. These nodes that stick together as a group for some time or for some common tasks. In every cluster the nodes elects a node as a cluster head which act as local DNS for own cluster and neighboring clusters.

EAACK Technique in Clusters:

Every cluster in the network can establish a enhanced adaptive acknowledgement technique in the their local region to finding the misbehavior nodes and limited transmission power problems and other collision problems within the node.

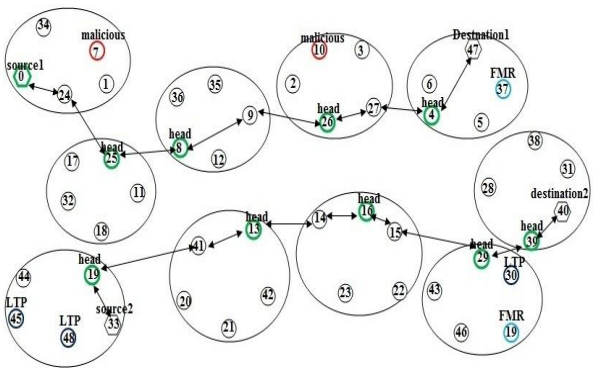

Fig: 6.Cluster based adaptive acknowledgement technique

After detecting intrusions with in every cluster it wish to transfer the data between two different nodes those belong to different clusters or same cluster. It can send the data through different nodes which are belong to different clusters by using simple end to end acknowledgment

scheme which was described earlier. This new IDS can avoid false misbehavior report and other intrusion problems. It can also avoid the forging of acknowledgement packets by greatly decreasing the number of acknowledgement packets; it can easily identify the malicious nodes before sending the data hence the forging of acknowledgement packet should not occur in the network.

The new arrival and elimination of nodes can be in the control current cluster head so it can't affect on the network performance. The packet delivery ratio and throughput of the network can be more efficient compared to other IDS systems. The simulation results can be seen in the following section.

IV. PERFORMANCE EVALUATION

In this section we can describe our simulation results by comparing with existing IDS system. The simulation methodology can be performing in NS2 with the maximum

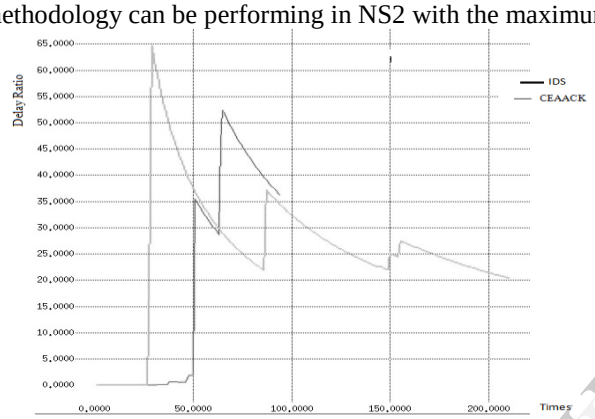

Fig: 7.Simulation results for delay ratio

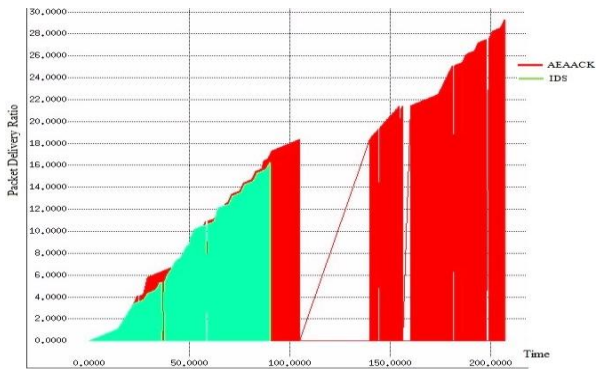

Fig: 9.Simulation results for packet delivery ratio

V. CONCLUSION & FUTURE WORK

The new IDS Enhanced Adaptive Acknowledgement technique can provide solution for the many problems from previous intrusion detection systems like false misbehavior report, reducing network overhead through large no of acknowledgement packets. By comparing this technique with previous IDS technique it produce good results in different metrics like packet delivery ratio,

of 50 nodes in the network. The physical layer and the 802.11 MAC layer are included in the NS2.

In order to see the performances of our proposed technique and the existing scheme we can use the following performance metrics.

1) Packets Delivery Ratio: It can be defined as the no of packets can be transferred in the network and the number of packet can be transferred between source and destination.
2) Packet Losses: The packet loss is the measure of loosing of packets in the network when packet transfer takes place in between nodes.
3) Delay Ratio: The delay ratio can be calculated as time taking to reach the packet from source to destination or in between nodes.

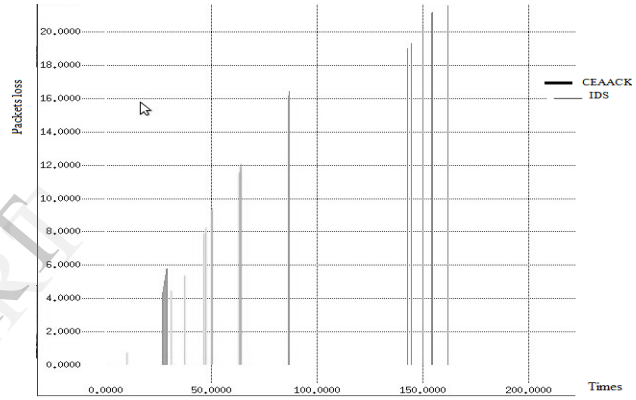

Fig: 8.Simulation results for packet loss

packet losses and delay ratio. This technique will use hybrid routing techniques like the combination of cluster based routing and AODV routing. Packet dropping attack and black hole attack can efficiently eliminate compared to other. The elimination of malicious and misbehavior of nodes can accomplished before sending the data through route and this elimination can takes place within the cluster or subnet.

We plan to implement our research work in some aspects:

1) By adopting the new routing schemes we can improve the performance and throughput of the network.
2) By providing the efficient clustering technology we decrease the packet losses in the mobile Adhoc networks.
3) Testing of CEAACK in real network environment compared to network simulation.

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: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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 Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[15] 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.

[16] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering Malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[17] 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.

[18] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[19] 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.

[20] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK—A Secure Intrusion Detection System for MANETs" IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013.

[21] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[22] 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-Verla g, 2011, pt. 3, pp. 384–387.