Techniques for Detection of Misbehaving Nodes in MANET: A Study

Rasika Mali, Sudhir Bagade

Abstract— Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes. MANET has variety of applications such military, disaster stuck areas and the characteristics like dynamic topology, no fixed infrastructure etc. Still there are some security issues and challenges in it. MANET is vulnerable to various attacks due to its open medium. Hence there is need to study in detail about how to detect malicious or misbehaving node present in network. In this paper we present different techniques for detection of misbehavior of node. Techniques studied in this paper are: Watchdog, ExWatchdog, TWOACK, S-TWOACK, 2ACK and Adaptive ACKnowledgment (AACK), CONFIDANT, Record and Trust Based Detection. All techniques are analyzed with parameters like type of misbehavior, key mechanism used, advantages, limitations and performance evaluation using packet delivery ratio (PDR) and throughput. We also suggested with the further research directions.

Index Terms— Acknowledgement Based Schemes, Attacks in Network, Intrusion Detection System, MANET, Misbehaving Nodes, Malicious Nodes, Reputation Based Schemes, Selfish Nodes .

1 INTRODUCTION

Mobile Ad hoc Network termed as MANET is collection of mobile nodes. Mobile nodes can be cell phones, PDAs, laptops etc. Every node in MANET has ability to transmit and receive data. Such mobile nodes in MANET can communicate with each other without fixed infrastructure. MANET can create its own self configuring and self maintaining network without centralized infrastructure. Basically there are two types of MANET: Close [1] and Open [1]. In closed MANET, all mobile nodes cooperate with each other for common goal. On the other hand in open MANET different mobile nodes having different goals share resources and hence ensure global connectivity. MANET has two types of networks, one is Single hop and another is Multi hop. There can be direct or indirect communication within nodes. In single hop network all nodes are within same range and can communicate directly which is known as direct communication but in multi hop network nodes rely on neighbors to communicate beyond transmission range which is known as indirect communication [2]. Communication in the network depends upon the trust on each other and communication can work properly if each node co-operate with another node for data transmission.

- *Rasika R. Mali, P.G. Scholar in Department of Computer Science and Technology, Usha Mittal Institute of Technology, SNDT Women's University, Mumbai, 400049, India*
  Email: malirasika4@gmail.com
- *Sudhir T. Bagade, Assistant Professor in Department of Computer Science and Technology, Usha Mittal Institute of Technology, SNDT Women's University, Mumbai, 400049, India*
  Email: bsudhiran@ieee.org

1.1 Characteristics of MANET

- Can be set up anywhere
- Dynamic Network Topology
- Wireless Communication Medium
- No need of centralized administration
- Nodes can perform the roles of both transmitter and receiver
- Autonomous in nature hence, no fixed infrastructure needed

1.2 Vulnerability in MANET

In spite of having variety of applications and number of characteristics stated above there are still some security issues and challenges in MANET. MANET is vulnerable to various attacks at its different layers. Due to its open medium, attackers can easily break into the network. All nodes in MANET are cooperative in nature but attackers may insert malicious or non cooperative node into network and compromise the security of network. Hence there is need of mechanism like intrusion detection system which will detect misbehaving node present in network.

1.3 Attacks in MANET

There are various attacks studied in the literature [3], [4] which is described below.

Denial of Service Attack: This attack limits access to a certain resource. The resource can be a specific node or service or the whole network. After successful attack service will not be available to the valid users.

Impersonation: Malicious node act as genuine node and then analyze network traffic. They are capable to send forged packets and get access to information.

Eavesdropping: Node observes confidential information like

location, public key, private key, password etc. This information can later be used by malicious node or eavesdropper to break the security of network.

Black-Hole Attack: A malicious node sends fake routing information and claims that it has an optimum route. It then causes other good nodes to route data packets through the malicious one. A malicious node drops all received packets instead of normally forwarding those packets to intended recipients.

Man-in-the-middle Attack: An attacker sits between the sender and receiver and sniffs any information being sent between two nodes.

Jamming: Jamming attack will be implemented by knowing the frequency of malicious nodes. Attackers initially determine frequency at which destination node is receiving signal from sender. It then transmits jam signal on that frequency to disturb the communication.

Wormhole Attack: Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This tunnel between two colluding attackers is called the wormhole.

Spoofing: Spoofing attack takes place when a malicious node misrepresents its own identity. It then alters vision of the sender and hence forces sender to change the topology.

Sinkholes: In a sinkhole attack, a compromised node tries to attract the data to it from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes.

1.4 Misbehavior of Nodes

In wireless sensor networks "Misbehavior" refers to node that does not behave in proper way and has an abnormal behavior. In other words, if behavior of node deviates from its specification or set of behaviors then the node is said to be misbehaving [5]. Misbehavior takes place in following ways:

- Delay Packets
- Drop Acknowledgements
- Delay Acknowledgements
- Drop packets and modify routing information
- Don't forward packet to save its own resources
- Forward control packets while dropping data packets

There can be various types of misbehaviors [5]. Some of them are listed below:

- Failed / Malfunctioned: A node malfunctions because of hardware and software problems, climate, radio channel, link breakdown, accidental physical damage.
- Selfish: Selfish nodes have passive misbehavior. Selfish nodes do not intend to directly damage other nodes and do not cooperate. It saves battery life for own communication. A selfish node is unwilling to spend CPU cycles and available network bandwidth to forward packets.
- Malicious: Malicious nodes have active misbehavior. Malicious node intentionally damages other nodes and interrupts network operations. A malicious node may drop the packets, modify the routing information. It may not give priority to battery power saving.

A MANET is vulnerable to various kinds of attacks and hence suffers from misbehavior of nodes. A node misbehaves means there is an intrusion present in the network. To detect intrusion in the network an Intrusion Detection System (IDS) is proposed. A basic function of IDS is to detect and report malicious activity in ad hoc network. It enhances security level in MANETs.

In this paper we discuss different techniques for detection of misbehaving nodes. Each technique has their own pros and cons. Techniques may vary while using routing protocols. Some may work on dynamic source routing (DSR) whereas other works on AODV.

The rest of the paper is covered as follows. In section 2 we covered literature survey of different techniques for detection of misbehaving node. Section 3 includes analysis of surveyed techniques and comparison of those techniques. In section 4 we covered conclusion and direction for further research.

2 Literature Survey

In this section we survey different techniques to detect misbhaving nodes in network. Techniques to be surveyed are: Watchdog [6], ExWatchdog [7], TWOACK [8], S-TWOACK [8], 2ACK [9], Adaptive ACKnowledgment (AACK) [10], CONFIDANT [11], Record and Trust Based Detection [12]. We also studied some different approaches to IDS [13] and an agent based approach [14] for detection of misbehaving nodes present in network.

S. Marti, et al in [6] proposed mechanism for detection of misbehaving nodes. Basically it describes two techniques, Watchdog and Pathrater [6]. Watchdog identifies misbehaving nodes and Pathrater helps routing protocols to avoid these nodes. Misbehavior observed in this paper is about data packet drop. Mechanism uses on demand Dynamic Source Routing (DSR) protocol. Watchdog technique detects malicious node by overhearing next node's transmission. Watchdog maintains a buffer of recently sent packets. Then it compares each overheard packet with the packet present in buffer. If match found, the packet in the buffer is removed. It then considers that the packet has been already forwarded. On the other hand, if a packet is present in the buffer for long time and watchdog overhears that the node failed to forward packet within predefined time then watchdog increases a failure counter of a node.

Each node will have its own failure counter when it fails to forward the packet. If the failure counter of any node exceeds a predefined threshold value then watchdog concludes that the node is misbehaving. It then sends a message to the source about misbehavior of a node. Pathrater uses the feedback given by Watchdog about misbehavior of nodes and avoid those malicious nodes in further transmissions. It also rates every path in its cache and chooses the path that doesn't include misbehaving nodes. Watchdog failed to detect misbehaving node in some of the scenarios like ambiguous collision, receiver collision, limited power transmission, false misbehavior reporting, collusion and partial dropping.

N. Nasser and Y. Chen [7] describes mechanism for detection of misbehaving nodes, known as ExWatchdog. ExWatchdog is extension to Watchdog technique. Using this mechanism, weakness of Watchdog mechanism has been overcome to some extent. When node sends a false report of other nodes and notify that they are misbehaving then malicious node could partition the network by claiming that some nodes following it in the path are also misbehaving. ExWatchdog system aim is to detect such nodes. The source node first searches a path having no malicious node in it from the routing table. If such path is not available, source node launches a Route Discovery to find another path. After this, source node sends the message using new path. The message contains source address, destination address, sum, malicious node address. After receiving such message, destination node searches its own table entry and check if there is a match between entries in a table. If it does not match entry in the table, it concludes that the node is malicious. Destination node then returns a message to the source and confirms that the report about malicious node is true. On the other hand, if match is found between entries in a table, destination node compares the sum field of the passing in message with one present in the table. If the two sums equal, means the node it is not malicious. Node forwards all packets received by source node. On the other hand, if the two sums are unequal, then node falsely reported as malicious might be really malicious. ExWatchdog could solve only the problem of false misbehavior reporting but other problems of Watchdog are still unsolved.

K. Balakrishnan and P. Varshney [8] describe two techniques, TWOACK and Selective-TWOACK. These techniques are basically implemented to resolve receiver collision and limited transmission problem. TWOACK is network-layer acknowledgment-based scheme. Misbehavior observed using this technique is about Acknowledgement Delay. In this technique every data packet is transmitted over three consecutive nodes along the path from source to destination. When node forwards a packet, routing agent has to verify whether the packet is received successfully by the third node. TWOACK scheme uses special type of acknowledgment packets, termed as TWOACK packets. These packets have same functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer. Along the route every third node sends back an acknowledgement packet for the received data packet. If TWOACK packet is not received within predefined time then nodes is reported as malicious and hence misbehaving links can be detected by acknowledging every data packet.
S-TWOACK (Selective-TWOACK) scheme is also network-layer acknowledgment-based scheme. It's a derivative of the TWOACK scheme and reduces routing overhead incorporated by TWOACK. In this scheme, there is no need of sending back TWOACK packet for every node. Rather a node waits for certain number of data packets to arrive. After arrival of certain number of packets node sends back one TWOACK packet and that packet will acknowledge multiple data packets that have been received up till now. Though above technique solves some of the problems of existing technique it adds some amount of unwanted network overhead due to acknowledgement process during packet transmission. It may degrade life span of entire network.

C. Nayak, et al in [9] describes, 2ACK scheme which is very similar to TWOACK [8] scheme. It speaks about routing misbehavior in MANETs. Routing misbehavior is that some nodes will take part in the route discovery and maintenance processes but refuse to forward data packets. The 2ACK scheme is a network-layer technique. This technique uses another type of acknowledgment packet, known as 2ACK, to detect misbehavior of node. Like TWOACK, it also works over three consecutive nodes. But 2ACK packet is sent back only for fraction of received data packets. On the other hand, in TWOACK, it is required to send TWOACK packet for every data packet received. 2ACK gives better performance than TWOACK while acknowledging packets. Routing overhead in network is significantly reduced due to 2ACK scheme. The 2ACK scheme has an authentication mechanism to assure genuineness of 2ACK packets. This is one of the major difference between TWOACK and 2ACK scheme. The 2ACK scheme suffers from false misbehavior report.

T. Sheltami, et al in [10] describes acknowledgement based approach for detection of misbehaving node. The Adaptive acknowledgment (AACK) is a network layer acknowledgment-based scheme. Technique assumes bidirectional communication in every link between a pair of nodes. AACK is made up of two techniques namely, TWOACK and ACK (i.e. end-to end acknowledgment scheme). This scheme works in two parts. First (i.e. ACK), source node sends data packet to destination node. After successful arrival of packet at destination it sends back an acknowledgement (ACK) packet. When source node successfully receives ACK packet, transmission between source and destination is successful. Otherwise source node will switch to second part of system i.e. TACK mode. Then it sends TACK packet and follow the process. AACK reduces the routing overhead of TWOACK and give same network throughput. Misbehavior detected using this technique is dropping of data packets while forwarding control packets. It fails to detect malicious nodes in presence of false misbehavior report and forged acknowledgements. It suffers from partial dropping attaS. Buchegger, et al in [11] discusses reputation based scheme for detection of misbehav-

ing node. The technique is known as CONFIDANT (Cooperation of Nodes: Fairness in Dynamic Ad Hoc Networks), which is actually a routing protocol. This technique is purely based on dynamic source routing (DSR) protocol. CONFIDANT mechanism has four working components, namely, Monitor, Reputation System, Path Manager and Trust Manager. Using Monitor component node can detect deviations of next node on source route. It can be done either by listening to next node's transmission or by observing behavior of route protocol. Alarm message is sent to the Trust Manager for giving warning information. It notifies about the misbehavior of node. Each node maintains Local Rating Lists. Such lists can be used in route request to avoid bad nodes along the route to destination. It also helps to ignore the requests from malicious nodes about forwarding packet. Rating is updated only if there is sufficient evidence of malicious behavior that is significant for a node and that has occurred a number of times, exceeding threshold [11]. Evidences can be taken either from Monitor Component or Trust Manager Component. CONFIDANT mechanism gives better performance while working with DSR protocol.

S. Subramaniyan and W. Johnson [12] proposed a reputation based scheme to detect selfish nodes. Technique is known as Record and Trust Based Detection Technique. This technique analyzes detection of selfish node during routing and packet dropping. Selfish node is verified for data packet drop and then checked for false reporting. In this technique trustworthiness of a node is evaluated based on their behavior. By building trust model for a node we can evaluate trust of its neighboring nodes. Trust scheme helps to detect abnormal behaviors of node. When nodes with selfish behavior are detected, neighboring nodes do not cooperate with such selfish nodes. Each node has a global trust state for all selfish nodes in network. The trust state is maintained in the form of Trust Table. Trust Table has two fields, node id and trust value. Trust state of node is updated after receiving new trust certificates. Evaluation of a certificate can be done by verifying response from every neighboring node Trust for a node can be calculated as follows. Collect the information such as Energy, Packet Count, and Queue Size from neighbors. It then generates report and need to validate report rules. Review the current trust value. Compare current trust value with threshold value. If current trust value is greater than threshold value then the node is detected as selfish node and this selfish node is added to Block List. When node misreports the data it has been added to blocked list. For each data packet transferred trust node will receive a trust report. Set of all selfish nodes can be obtained from network by repeating above process. From analysis it is concluded that detection time is diminished and overall overhead is very low hence, this method of selfish node detection is very efficient. It also enhances packet delivery ratio, reduces average packet drop ratio hence reduces overall overhead.

M. S. Alnaghes and F. Gebali [13] present a survey of the different Intrusion Detection Systems (IDSs) that are proposed for MANETs. It also covers comparison of each IDS including their advantages and disadvantages. Paper discusses three types of IDS namely, Anomaly-based IDS, signature-based IDS and Specification-based IDS. As it is clear, it is difficult to build a completely secure MANET system in spite of using a complex cryptographic technique or secured routing protocols. Some of the existing IDS algorithms that have been introduced for MANETs are Bayesian Game Approach IDS, Acknowledgment-Based Approach IDS[9], Ex-Watchdog Approach IDS[7], Classification-Based Approach IDS, Zone-Based Approach IDS, Fuzzy Logic Approach IDS, Elliptic Curve Cryptography-Based Enhanced Adaptive Acknowledgment IDS, Cross Layer-Based Approach for IDS. Bayesian Game Approach IDS is a game theoretic framework built using a Bayesian formulation which can analyze the interactions between pairs of attacking and defending nodes was introduced in a flat Ad-hoc network. Thec2-ACK scheme [9] is one of the Acknowledgment-Based IDS. It forwards two hop acknowledgment packets in the opposite direction of the routing path. This approach is an add-on method for routing schemes to detect and mitigate the effect of such routing misbehavior. Ex-Watchdog intrusion detection system [7] is an extension of Watchdog System [6] whose function is to detect intrusion from malicious nodes and reports this information to the response system. Classification-Based IDS models using supervised classification algorithms. The used classification algorithms are Multi-Layer Perceptron (MLP), the linear classifier, the Gaussian Mixture Model (GMM), the Naive Bayes and Support Vector Machines (SVM). IDS architecture composed of multiple local IDS agents that are responsible for detecting possible intrusions locally. Zone-Based intrusion detection system is a non overlapping zone-based framework. The use of different detection techniques is pliable in their IDS agents, but technically they only use Markov chain anomaly detection in their research. In fuzzy logic based IDS, fuzzy logic works to handle imprecise information in order to help the IDS to detect malicious behavior and identify the attacks. An acknowledgment-based IDS named Elliptic Curve Cryptography Based Enhanced Adaptive Acknowledgment demonstrates higher rates for malicious behavior detection in certain situations while does not greatly affect the network performances. A cross layer-based detection system detects the black-hole attack in MANETs. This technique incorporating IDS leads to an escalating detection rate in the number of malicious behavior of nodes increasing the true positive and reducing false positives in the MANET.

Sumiti and S. Mittal [14] proposed a distributed agent based technique for detection of passive path selfish node in mobile network. Several intrusion detection systems have been proposed to find out misbehaving nodes in MANETs, which are classified into three categories, Credit Based System, Reputation Based System and Acknowledgement Based System. This paper also discusses different techniques to detect misbehavior of node. Those techniques are Watchdog and Pathrater scheme [6], CONFIDANT protocol [11], TWOACK [8] and 2ACK [9]. In proposed Agents based technique, agents are designed for gathering the information from various nodes.

Every node is like a watch module whose task is to check the neighboring nodes, observe their behavior and check out whether the node is selfish or not. Each node sends the message to its adjacent first hop neighbor's node. Every node in the mobile ad hoc network participates in the detection activities. Neighboring nodes share their investigation results with each other and cooperate in a broader range. After that the agent runs an observation technique to get the conduct data from the neighboring nodes. The system encourages the cooperating nodes for providing quick service. Agent builds a table for selfish and normal operating node. Agent uses coordination, cooperation, rating mechanism and evaluating mechanism to detect selfish node. After detecting this selfish node; the path is changed and a new path is followed. This technique isolates the selfish node in an efficient manner but adds some overhead while detecting and coordinating new path between nodes.

3 Analysis of Surveyed Techniques

Watchdog mechanism detects misbehavior of node, if there is large delay in packet transmission. It fails to detect misbehaving node under various circumstances like partial dropping, receiver collision, false misbehavior reporting. Similarly, by listening to next node's transmission, Confidant technique also detects misbehaving node. Watchdog simply avoids bad nodes along the route. On the other hand, CONFIDANT technique not only avoids those nodes but also reject forwarding requests from those nodes. ExWatchdog is extension to Watchdog and solves problem of false misbehavior reporting while other problems of watchdog are still unsolved. Misbehavior detected using this technique is in terms of dropping of packets.

Record and Trust Based Detection Technique detects selfish nodes for data packet drop and false reporting. TWOACK, 2ACK and AACK are purely acknowledgement based approaches that take place at network layer. A TWOACK and 2ACK technique detects similar type of node's misbehavior which is in terms of delayed acknowledgment. AACK detects packet dropping.

In Table 1 we summarized different techniques for detection of misbehaving nodes in network. All techniques are compared using parameters like type of misbehavior, key mechanism used, advantages, limitations and performance evaluation using packet delivery ratio and throughput. Techniques like Watchdog, ExWatchdog and Confidant has more disadvantages than others.

Watchdog mechanism increases network throughput by 17%-7% in presence of malicious nodes. ExWatchdog increases throughput by 11% more than that of Watchdog. TWOACK has large network overhead and AACK reduces network overhead by adoption of hybrid scheme but PDR of both schemes is increased by 15%-20%. 2ACK mechanism significantly reduces routing overhead and PDR is almost 91%. Record and Trust Based Detection technique enhances packet delivery ratio by 18%, reduces average packet drop ratio and thereby reduces overall overhead. CONFIDANT mechanism increases PDR by 9%-10%.

4 Conclusion and Further Research

In this paper we surveyed various techniques to detect misbehavior of nodes in MANET. We also studied various attacks possible in MANET. Then we studied types of misbehavior a node can have and different ways to misbehave. Each paper surveyed is in terms parameters like type of misbehavior, key mechanism used, advantages, limitations and performance evaluation using packet delivery ratio and throughput. Techniques surveyed in this paper are Watchdog, ExWatchdog, TWOACK, S-TWOACK, and 2ACK, AACK, CONFIDANT, Record and Trust Based Detection. We also studied an agent based technique for detection of selfish nodes in a path which is efficient detection technique but adds routing overhead in network. Watchdog has good network throughput, but suffer from various disadvantages which are resolved to very little extent by other techniques. ExWatchdog solves the problem of false misbehavior reporting. With DSR protocol, CONFIDANT mechanism gives better performance. Record and Trust Based Detection technique enhances packet delivery ratio, reduces average packet drop ratio and overall overhead. 2ACK and AACK have reduced routing overhead and reduced network overhead respectively.

Still the problem of receiver collision, limited transmission power and partial dropping are unsolved and need to be solved by new techniques in future. There are some other kinds of misbehavior namely; 1) Drop packets and modify routing information 2) Don't forward packet to save its own resource 3) Delay Packets; which are still not detected by any of the techniques we studied. So there is a need of detecting such type of misbehaviors in highly secured MANETs. Providing security to data being transferred over network is highly recommended. By using cryptographic algorithms it is possible to make data secure and non vulnerable.

TABLE 1
SUMMARY OF COMPARISON OF TECNIQUES

Technique	Type of Misbehavior	Key Mechanism Used for Detection	Advantages	Limitations	Performance Evaluation
Watchdog 2000 [6]	Drop Data Packets	Listen to its next hops transmission	Improve network throughput with presence of malicious nodes	Receiver collision Limited Transmission Power False Misbehavior Report Ambiguous Collision Partial Dropping	Throughput Increased by 17% - 27%
ExWatchdog 2007 [7]	Drop Data Packets	Detects a node that sends false reports	Solves problem of false misbehavior report	Receiver Collision Limited Transmission Power Ambiguous Collision Partial Dropping	Throughput increases by 11% more than Watchdog
TWOACK 2004 [8]	Acknowledgement packet Delay/ Drop	Acknowledge every data packet transmitted over every three consecutive nodes	Detects misbehaving Links	Adds overhead in the network May degrade life span of entire network	Packet Delivery Ratio Increased by 15% - 20%
2ACK 2011 [9]	Forwards control packets and Drops data packets	2ACK packet is sent back only for fraction of received packets	Routing overhead is significantly reduced	Suffers from false misbehavior report	Packet Delivery Ratio is almost 91%
AACK 2009 [10]	Forwards control packets and Drops data packets	Combination of TACK and end to end acknowledgement i.e. ACK scheme	Reduces network overhead due to adoption of hybrid scheme	Does not guarantee validity and authenticity of acknowledgement packets	Packet Delivery Ratio Increased by 15% - 20%
CONFIDANT 2014 [11]	Drop Data Packets	Listen to its next hops transmission	Avoid misbehaving nodes and any request from them in future transmission	Same as Watchdog	Throughput Increased by 9% - 10%
RTBD 2014 [12]	Drop Data Packets	Trustworthiness of a node is evaluated	Overall overhead is very low	No security for neighboring nodes	Packet Delivery Ratio Increased by 18%

REFERENCES

[1] Arockia Rubi and Vairachilai "A Survey on Intrusion Detection System in Mobile Adhoc Networks," *International Journal of Computer science and Mobile Computing*, vol. 2, Issue 12, Dec. 2013, pp. 389-393.

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

[3] Zaiba Ishrat "Security Issues, Challenges and Solution in MANET," *International Journal of Current Science and Technology*, vol. 2, Issue 4, Oct. - Dec. 2011.

[4] J. Godwin Ponsam, Dr. R.Srinivasan "A Survey on MANET Security Challenges, Attacks and its Counter-measures," *International Journal of Emerging Trends and Technology in Computer Science*, vol. 3, Issue 1, Jan.–Feb. 2014.

[5] I. Hatware, A. Kathole, M. Bompilwar "Detection of Misbehaving Nodes in Ad Hoc Routing," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, Feb. 2012.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, 2000, pp. 255-265.

[7] N. Nasser and Y. Chen "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network," in *Proceedings of the IEEE International Conference on Communications*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[8] K. Balakrishnan, Jing Deng and P. Varshney "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," *M.S. Thesis, Department of EECS*, Syracuse University, Syracuse, NY, USA, Aug. 2004.

[9] C. Nayak, G. K. Dash, K. Parida and S. Das "Detection of Routing Misbehavior in MANETs with 2ACK Scheme," *International Journal of Advanced Computer Science and Applications*, vol.2, no. 1, Jan. 2011.

[10] T. Sheltani, A. Al-Roubaiey, E. Shakshuki and A. Mahmoud "Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs," *Journal of Multimedia Systems*, Springer, Oct. 2009.

[11] S. Buchegger, J. Y. Le Boudec "Performance Analysis of the Confidant Protocol (cooperation of nodes: fairness in dynamic ad hoc networks)," in MobiHoc'02, *IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2002.

[12] S. Subramaniyan, W. Johnson and K. Subramaniyan "A Distributed Framework for Detecting Selfish Nodes in MANET using Record- and Trust-Based Detection (RTBD) Technique," *EURASIP Journal on Wireless Communications and Networking*, Springer, 2014.

[13] M. S. Alnaghes and F. Gebali "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks," *In Proceedings of Second International Conference on Electrical and Electronics Engineering*, Clean Energy and Green Computing, Konya, Turkey, 2015.

[14] Sumiti, S. Mittal "Identification Technique for All Passive Selfish Node Attacks in a Mobile Network," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, Issue 4, Apr. 2015.