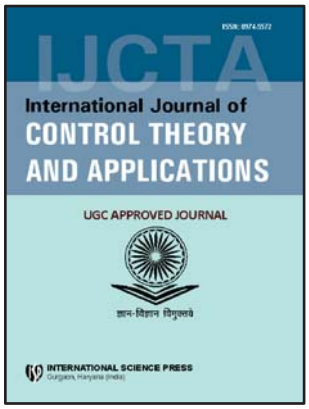

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 30 • 2017

Security Based Duplication Data Removal for Packet Transmission in Manet

J. Wilson[a] and Kamalraj Subramaniam[b]

[a]*Research Scholar, Department of ECE, KarpagamUniversity.*

[b]*Associate Professor, Department of ECE, KarpagamUniversity.*

Abstract: Mobile nodes positions are free of nature. It tracks along the network environment concurrently. Mobile node initiates to broadcast data packets in general way minimum quality of data packet get captured by destination node, also analyze node characteristics. Attacker node misuse original information for packet transmission, and also it provide fake information so duplicate data received, they affect network lifetime. Proposed a Security Based Duplicate Data removing technique (SBDD), to enhance packet transmission, it easily detect the wrong data from packet and removed it before perform communication. Data dribbling algorithm is used, it filter outs wrong data information, this scheme is applied to all nodes present in routing path, it easy to find and remove intruded data packets then finally forward only original data to destination node. This technique supports to perform intrusion free communication. It improves throughput rate, network lifetime, and minimize packet loss rate.

Keywords: *Security based duplicate data removing technique, Data dribbling algorithm, Original data forwarding.*

1. INTRODUCTION

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain.

The ultimate goal of the security solutions [1] for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. In this article we consider a fundamental security problem [2] in MANET: the protection of its basic functionality to deliver data bits from one node to another. In other words, we seek to protect the network connectivity between mobile

nodes over potentially multi-hop wireless channels, which is the basis to support any network security services. Multi-hop connectivity is provided in MANETs through two steps: (1) ensuring one-hop connectivity through link-layer protocols like wireless Medium Access Control (MAC), etc., and (2) extending connectivity to multiple hops through network layer routing and data forwarding protocols like ad hoc routing. Accordingly, we focus on the link- and network-layer security issues, challenges, and solutions in MANETs in this article.

One distinguishing characteristic of MANETs from the security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols, such as Ad Hoc On Demand Distance Vector (AODV) [3] and Dynamic Source Routing (DSR) [4], and wireless MAC protocols, such as 802.11 [5], typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: routing attacks and packet forwarding attacks, based on the target operation of the attacks.

The specific attack behaviors are related to the routing protocol used by the MANET. For example, in the context of DSR [6], the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list [7]. When distance-vector routing protocols such as AODV [3] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [8]. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even nonexistent.

The main aid of this work is detecting the attacks and reducing it to improve the security of MANET. In this work, a security based duplicate data removing technique is proposed based on Data dribbling algorithm. In transmission process, before sending the packet, it can be checked, if it is affected or not. If affected means, it can be removed and then transformed to destination node using the dribbling algorithm. Residual of the paper is planned as follows. Section II indicates a related works. In section III, we present the details of proposed security based duplicate data removing technique based on Data dribbling algorithm to provide security for MANET. Section IV provides simulation performance results analysis obtained under different parameters. Finally section V concludes the paper with future track.

2. RELATED WORKS

In 2011, Denko et al. [9] investigated a probabilistic trust management scheme to be implemented in pervasive computing environments. The authors argued that in addition to allowing a device to find other suitable devices for interaction, while detecting those that were malicious. This trust model was capable of allowing a device to judge the trustworthiness (*i.e.* reliability) of another device with which it interacts by means of the recommendations from its peers. The behavior changes as expected depending on the proportion of malicious devices, and when a device gains enough experience of interactions with other devices in the environment, it starts to protect against false recommendation attacks depending on the proportion of false recommenders.

In 2011, Muktikanta Sa et al. [10] developed an algorithm for detecting the misbehaviour of the node based on the Bayesian methodologies. The authors analyzed their performance improvement based on their agent based approaches over the conventional methods.

In 2011, Jian-Ming Chang et. al. [11] proposed Cooperative Bait Detection Scheme (CBDS) which is able to detect and prevent malicious nodes launching cooperative black hole attacks. It integrates with the proactive and reactive defense architectures and the source node randomly cooperates with a stochastic adjacent node. When source node initializes Route Discovery, it sends out the bait RREQ' and then source node receives RREP. If RREP is from not existed destination node or intermediate node then trace which node sends back the RREP according to RREP packet's Record address field. The location of black hole is recognized and detected by source node when receiving the fake RREP. Then the detected black hole node is listed in the black hole list and noticed all other nodes to revoke the certificates of black hole by propagating Alarm packets through the network. Ignore any responses from black hole are discarded.

In 2012, Fenye Bao et al. [12] proposed a novel system to identify the malicious nodes using clustering approach which based on trust system. In this work, the authors derived the properties of each node in the wireless environment system to classify the nodes behaviours in an effective and simple manner. The authors developed probability distribution density function for the nodes in heterogeneous network and each node in the wireless network environment derives the quality of service (QoS) properties. Nodes were classified based on this derived set of features. The authors also designed a reputation-based framework to ensure data integrity in WSNs, which collects information from each node by means of a Watchdog technique which identifies the malicious nodes or hidden nodes in structured or unstructured wireless sensor network environment.

In 2013, Bo Sun et al. [13] presented an anomaly detection technique for Wireless Sensor Networks. By means of various aggregation functions like sum, average, max, and min, the authors presented how to obtain a theoretical threshold. The authors implemented an algorithm to increase detection sensitivity by the integration of generalized likelihood ratio and cumulative summation. The authors proposed a new system integrating both system monitoring modules (SMM) and intrusion detection modules (IDM) for implementation in Wireless sensor networks. This combination helps to classify the malicious events and other emergency events. In practice, WSNs are made use in monitoring significant emergency events, such as battlefield monitoring and forest fires.

In 2014, Gopalakrishnan and Ganeshkumar [14] have proposed different detection methods for attackers who hacked the packets in networks. The authors proposed Secure Routing for Attacker Identification (SRAI) protocol to detect and mitigate the attackers in the network environment. This proposed system automatically detected the attacks in the network and thus periodically generates the attacker identification report. This report was sent to all the nodes in the network environment and thus the attacks were identified in each node of the network.

In 2015, Chang et al. [15] devised a methodology to classify the nodes behaviour based on their cooperative bait approaches which predicted the attacks in the network. The problems of the conventional malicious node detection system were tolerated by implementing cooperative bait detection scheme (CBDS).The anomaly nodes were detected based on fuzzy theory and revised evidence theory. The malicious nodes in a network can be identified by monitoring the behaviors of the evaluated nodes with multidimensional features and integrating this information, thus, the normal operation of the whole network can be verified.

In 2015, Renyong Wu et al. [16] proposed an anomaly node detection in networks using trust based authentication algorithm. The anomaly nodes were detected based on fuzzy theory and revised evidence theory. The frequent observation and integration of the behavior of the evaluated nodes with multidimensional characteristics helps to detect the malicious nodes in a network. The authors also devised a system which detected intrusion based on Neighbor Node Trust algorithm. Each node examines the trust level of its neighbor nodes. Depending on the obtained trust values, the neighboring nodes may be classified into risky, malicious

or trustworthy. Trustworthy nodes were recommended to the forwarding engine for the purpose of packet forwarding. Their scheme successfully detected HELLO flood attack, selective forwarding attack, and jamming attack by analyzing the malicious node behavior and other network statistics.

In 2015, Haripriya et al. [17] proposed a framework to detect and mitigate the malicious nodes. The authors detected the malicious nodes in prior to the routing using consensus based algorithm and then that route is prevented for transmitting data between nodes in mobile adhoc networks.

In 2016, Pradnya M. Nanaware et al. [18] presented trust system based intrusion detection in mobile ad hoc network. In this paper the trusted nodes are separated and those nodes can only be used in the communication and quality of the network can be improved. The trust improvement is important minimize the biasing and maximize the performance of the network. The bias minimization is important to proper selection of the node for communication. Less biased nodes can be selected for good quality of the network. As the trusted nodes are selected for the communication, the performance of the network improves.

In 2016, Andrea Lupia et al. [19] proposed a Trust Management using Probabilistic Energy-Aware Monitoring for Intrusion Detection in Mobile Ad-hoc Networks. The adoption of Intrusion Detection System (IDS) to discover internal attacks is often energy consuming highly reducing the network lifetime. At this purpose, the proposal is the design and adoption of an energy-aware probabilistic monitoring module useful to IDS, to better perform in a MANET scenario where not only security but also energy constraints need to be accounted. The proposed scheme has been analyzed by an energy point of view and considering also its efficacy to discover malicious nodes under different network conditions.

3. OVERVIEW OF PROPOSED SCHEME

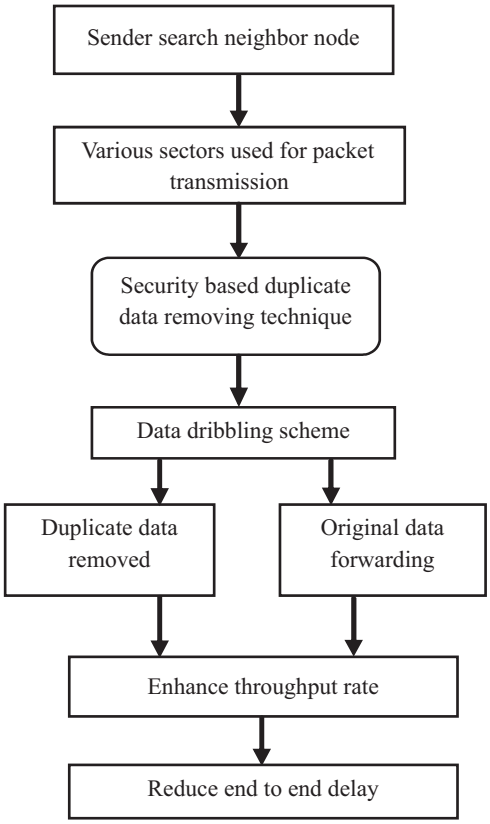

Figure 1: Block Diagram of Security based duplicate data removing technique

Mobile network perform packet sharing lot of interference occurred, since its behavior is changed at every time, wrong information is inserted to the packet before starts communication, to capture those original information they are misused, so energy consumption is increased that makes the connection failure at every situation.

Normally mobile source node monitor environment and get some information they are transmitted to various groups, to split nodes in path at various sectors, those sectors are perform packet transmission, authentication is important one to improve delivery ratio, it contain data dribbling algorithm to detect and remove wrong information in packets. It filters out duplicate data and only maintains original data. It applied to each node present in routing path, improves throughput rate.

Figure 1 shows Security based duplicate data removing technique. Different sectors are used to construct in routing path to broadcast data packets frequently from sender node to destination node along routing path. Security based duplicate data removing technique is applied to Mobile network. it contain data dribbling algorithm to remove the duplicate data and forwarding original data packet to destination node. It improves throughput rate and reduce end to end delay.

Wrong data's in packets are ignored for every transmission, Data dribbling perform important role in communication between sender and receiver node in mobile network. The data packets are normally secured, but its information is varied based on nodes visited for packet transmission.

3.1. Splitting nodes to various sectors

Lot of sectors in routing path from its sender node to its target node is a sequence of packet broadcasting and storing of the information by the relaying nodes. There is traffic free communication performed in routing path. Packets travels along allocated path decayed into self-sufficient sectors. All sectors having packet latency make by the process carried relay node on the route. Specify that because nodes travels in any node perform communication can be packet broadcasted with other intermediate node. Consequently, the possibility sharing of a route only based on quantity of nodes then not considers the position of nodes on the route. Triple kinds of sectors from sender node to destination node Sending data the packet directly to the destination node, below the situation that this node is establish in neighbor node's coverage range.

An additional condition some nodes interfere to another communication coverage range in a direct routing path. Those conditions node consume more power, because the standard distance between different target nodes in path. The same command of the surface distance of the network route. This condition is not checked for minimum values of velocity because nodes updates route within little ladder. However, indicate in result, it maintains node velocity values in every time and denote current situation.

Mobile nodes move in various directions to monitor its characteristics and establish communication among sender node to destination node. Intermediate sector node operates in a normal manner analog amplify to the captured data packet from initial sector node, depends on path evaluation, need to broadcast this information to the destination node. Sector technique is launched to monitor particularly in different process. It is proposed to monitor behavior they are dual type of analog relaying: unknown and known position of relay nodes in network. While unknown position of relay node is monitored and experimental result shows the all node performance.

Ordinary packet transmission scheme is used to analyzing the misbehaving characteristic nodes in routing path, it contain an extra significative summary against the connection superiority. Packet sharing scheme theme to a random disappearing is the numerical average result of the immediate representation fault result. Allowing for an indication prearranged by paths, different sectors Mobile network under Wireless Mesh Networks and presents Security based duplicate data removing as the already construct the different path finding rules. Previous investigation method focusing authentication, during packet transmission period among sender node to destination node in mobile network, but added new scheme is wrong data detection it analyze the node capacity. To transmits data packets frequently along routing path with higher efficiency.

All nodes can loss the packet exchange in both directions between neighbor nodes. From end to end this overloading process, the data's of one-hop neighbor for a certain sender node to target node in routing path is resolute. Split the routing path nodes into different sectors applied on mobile nodes, Traffic in all way of packet transmission for the same sender node to target node in allocated time slot. The single hop intermediate node estimate the cost to reach the target node from the traffic occurrence and revise node storage area. Single hop relay node alters the routing table data's such as resource utilization and various metrics.

3.2. Security based duplicate data removing technique

The sender node searches the kindness of the nearest neighbor node to attain the target node and it is the wrong way round relative to the communication rate Single hop intermediate relay node broadcast data packet within allocated time, details of resource utilization is measured to enhance packet transmission at high speed to attain target node of the traffic rate, sender to target node join up in a request hello packet. Whether some nodes capture the packets they alter the resource utilization rate to the target node. Those data's are stored by the pheromone spreading function is place to stationary path because they are achieved by overload. Pheromone spreading depends on request packet is unfinished only to the one hop relay node by traffic occurrence; the entire positive traffic rate is minimized.

All nodes are deployed at different way in the environment starting that modernizes the location of target node. The centres of the environment, each sector are divided into two sectors to diversion the stack that might be model as an intended output to the lesser likelihood to merge nodes. The middle checkpoint, double clusters are combined and the directive belong to the combine sectors.

$$\mathrm{P}ki1 = \tan(\phi\, kip) \tag{1}$$

$$\mathrm{P}kij = \cos(\phi\, ki(j-1)) + 1\tan(\phi\, \mathrm{kip}) \tag{2}$$

$$\mathrm{P}kin = \cos(\phi\, ki(j-1)) \tag{3}$$

The node need to create wrong data packets that is forwarded to each neighbor node using the intruder node. Wrong data packet removes each path with connection between sender node to target node. Leading capturing notice of a connection blocked, sender node remove the failure route from its main route collection and looks up its next path collection for several distance path to the target. Whether it identify single hop straight away, to broadcast information about path condition, among nodes present in routing path.

Target node need to give reply packet to source node they are investigate message. Investigate messages support to preserve the dependability of data transmitted successfully. Receiving of a response message the sender then encourage the already hold route as the initial route and begin packet sharing with the target node. Though whether the senders not succeed to capture response investigate message while a few investigate message response stay long period, it starts a latest path finding function. Wrong packets are deleted from the collection whether they are not used for a particular quantity of time period.

$$\mathrm{P}k = (\mathrm{P}kij\ /\mathrm{P}kin) \tag{4}$$

$$\mathrm{P}k = ((\cos(\phi\, ki(j-1)) + 1\tan(\phi\, \mathrm{kip})/\cos(\phi ki(j-1))) \tag{5}$$

To achieve and preserve node link details, all node is need at regular intervals transmit a single hop request packet to its intermediate relay nodes. While a node captures a request packet from remaining node does not contain nearest neighbor node records, it inserts that node to its neighbor record as original intermediate node. Also whether a node not succeed to capture request packet from a intermediate node before in its region when three successive request time gap the connection to the neighbor in queries are accepted. Whether the node indicates out of order connection is element of a present path, the path preservation scheme is invoke. Entrenched in the request packet is an open broadcasted. While this group shows that the intermediate node is experiencing sharing rules.

Security based duplicate data removing algorithm

Step 1: For each sender broadcast data packet to target node

Step 2: Different sectors are used to forward those data packets

Step 3: If {Packet == original data}that are broadcasted

Step 4: Neighbor node send to destination node minimum energy is used.

Step 5: Else

Step 6: If{packet == duplicate data} that are filtered.

Step 7: Remove duplicate data before forward to next neighbor node.

Step 8: End if

Step 9: Minimize energy consumption.

Step 10: End for.

3.3. Data dribbling scheme

Present rules data dribbling scheme is energy aware method, traffic removal and not be easily influence by relay node in routing path. Designing needs individually would output in a difficult rules containing an unfavourable cause on the entire network characteristics. Consequently to maintain the rule is easy and well-organized, individual path finding parameters that cannot be easily manipulate by misbehaving nodes and that reproduce both network packet more traffic and energy sharing. Still though amount of packets waiting in the node's row can be used to calculate the overloading, it is not minor to create a capable cost purpose that merges the storage in sequence with the residual sequence authority. The overload at a node as the number of action in particular node, the amount of packet broadcasted, captured and overload when examine period.

The sender node of power usage, with regard to network performance, it is divided into two parts: packet based and calculation based. In order to construct simpler performance and dissimilarity to invent as steady the calculation based energy usage. The power utilized for time gap with packet sharing based performance.

Lifespan of node is a straight process of the residual battery capability and an opposite process of the overload, because lifespan of node is state as a process of both the energy condition and the over load situation at each node. Consequently used to choose path, parameters are both energy and traffic free. To construct this path finding parameter a node analyzes its energy capability and after every consecutive period gap evaluates the energy loss with network lifespan. This process can be comprehensive to obtain route lifespan, most excellent path lifespan to coolness path lifespan at the target node.

Data dribbling algorithm

Step 1: Neighbor receive data packet to perform dribbling.

Step 2: If {Dribbling == wrong data}

Step 3: There is any fake data occurred to remove them from packet

Step 4: To increase network lifetime

Step 5: Else

Step 6: If {Not Dribbling == correct data}

Step 7: They are broadcasted to next neighbor node.

Step 8: Throughput is enhanced

Step 9: End if.

Higher route finding parameters can analyzed in presents of bad data inserted by misbehaving node in network environment. Whether a misbehaving node provides a lesser otherwise higher lifespan, when route details are gathering phase, discovery of a path by the target node cannot be authority by individual node active rate. It assures the quantity of protection in the mobile network.

Packet ID: Packet ID includes entire mobile adhoc network data's. This comprises of every status updates of nodes and node's position.

Source ID	Destination ID	Splitting nodes to various sectors	Remove duplicate data with security	Data dribbling	Original data transmission
2	2	4	4	4	2

Figure 2: Proposed Packet format

In figure 2: the present packet format is furnished. Now the source and destination node ID field takes 2 bytes. This is given in first and second field. Third field is splitting nodes to various sectors that occupy 4 bytes. The fourth field is for removing the duplicate data that is attained with security. This field occupy 4 bytes. In fifth field it occupies 4 bytes which is for data dribbling. At last, sixth field is for forwarding original data that occupies 2 bytes. This removes the duplicate data and transmits only the correct data. Hence it enhances the throughput and network lifetime.

4. PERFORMANCE EVALUATION

4.1. Simulation Model and Parameters

The proposed SBDD is simulated by using Network Simulator tool (NS 2.34). In simulation, sensor nodes of about 100 nodes are deployed in the square region of 1050 meter x 900 meter for 80 milliseconds simulation time. Each sensor nodes are deployed in arbitrary manner among the network. Every node has the similar transmission range of 250 meters. CBR Constant Bit Rate provides a constant speed of data communication in network to limit the traffic rate. DSR Dynamic source routing protocol is employed to cover and stitch every packet before transmission. Table 1 shows Simulation setup.

Table 1
Simulation Setup

No. of Nodes	*100*
Area Size	1050 X 900
Mac	802.11
Radio Range	250m
Simulation Time	30ms
Traffic Source	CBR
Packet Size	150 bytes
Mobility Model	Random Way Point
Protocol	DSR

Simulation Output:

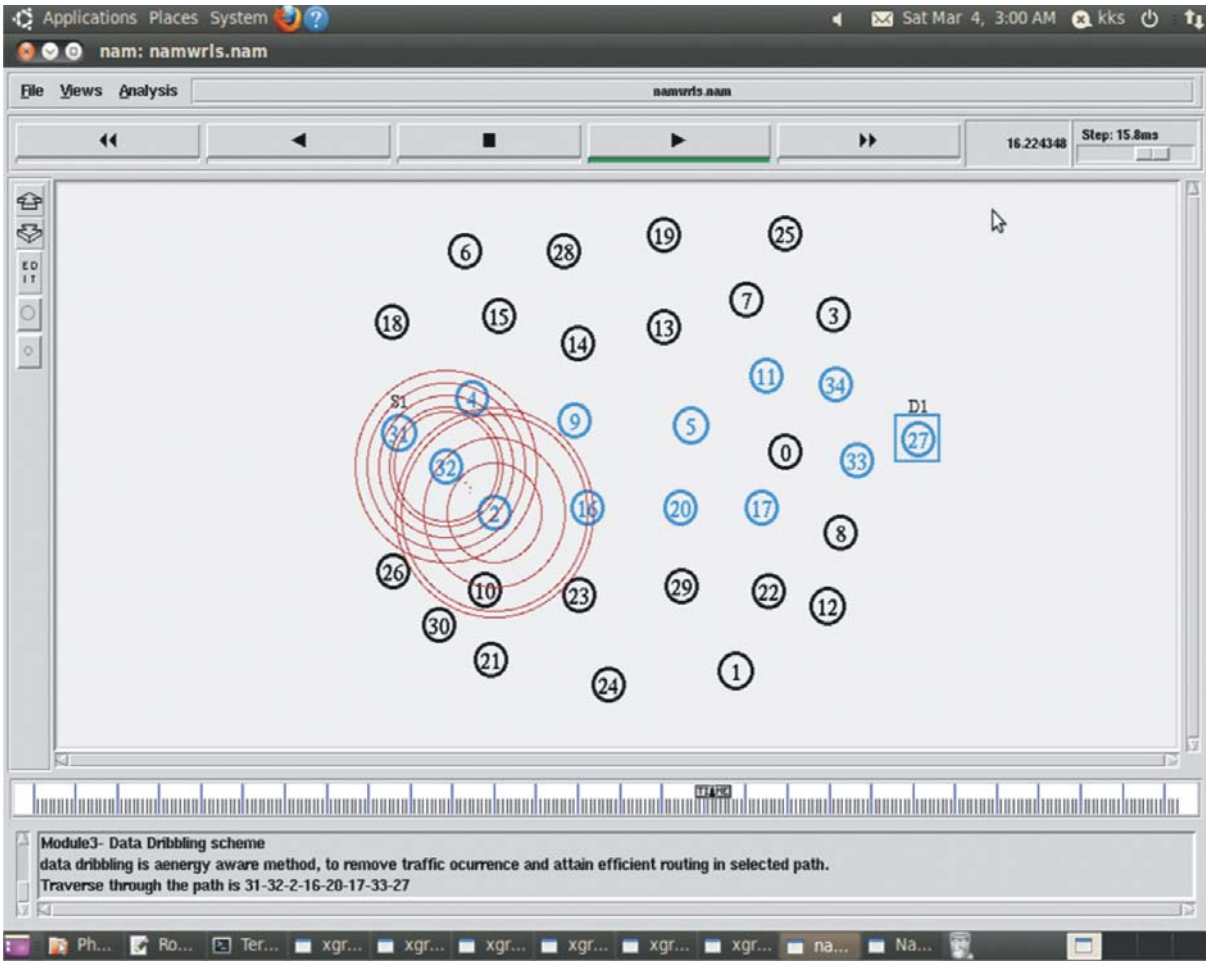

Figure 3: Proposed SBDD Result

Simulation Result: Figure 3 shows that the proposed SBDD scheme improves the transmission of packet compared to the existing methods ITBS [19] and NAGH [20]. Present SBDD method supports to implement intrusion free transmission by filtering out the incorrect data information. This method is executed in every node in the routing route and can find out intruded data packets easily and remove it and transmits the original data alone. This maximizes the lifetime of network, throughput rate and reduces the loss of packets.

4.2. Performance Analysis

In simulation to analyzing the following performance parameters are using X graph in ns2.34.

Average Delay: Figure 4 shows average delay which is computed by measure of time utilized for transmission of data from sender node to seed node, behavior of node are examined by anchor node. In proposed SBDD scheme average delay is reduced compared to Existing methods ITBS and NAGH.

$$\text{Average Delay} = \text{End Time} - \text{Start Time}$$

Network overhead: Figure 5 shows network overhead is decreases that sender node requires transmitting packet to anchor node to filter out error data packets, all packets are covered and stitched efficiently. In proposed SBDD scheme network overhead is minimized compared to existing methods ITBS and NAGH.

$$\text{Network overhead} = (\text{Number of Packet Losses/Received})*100$$

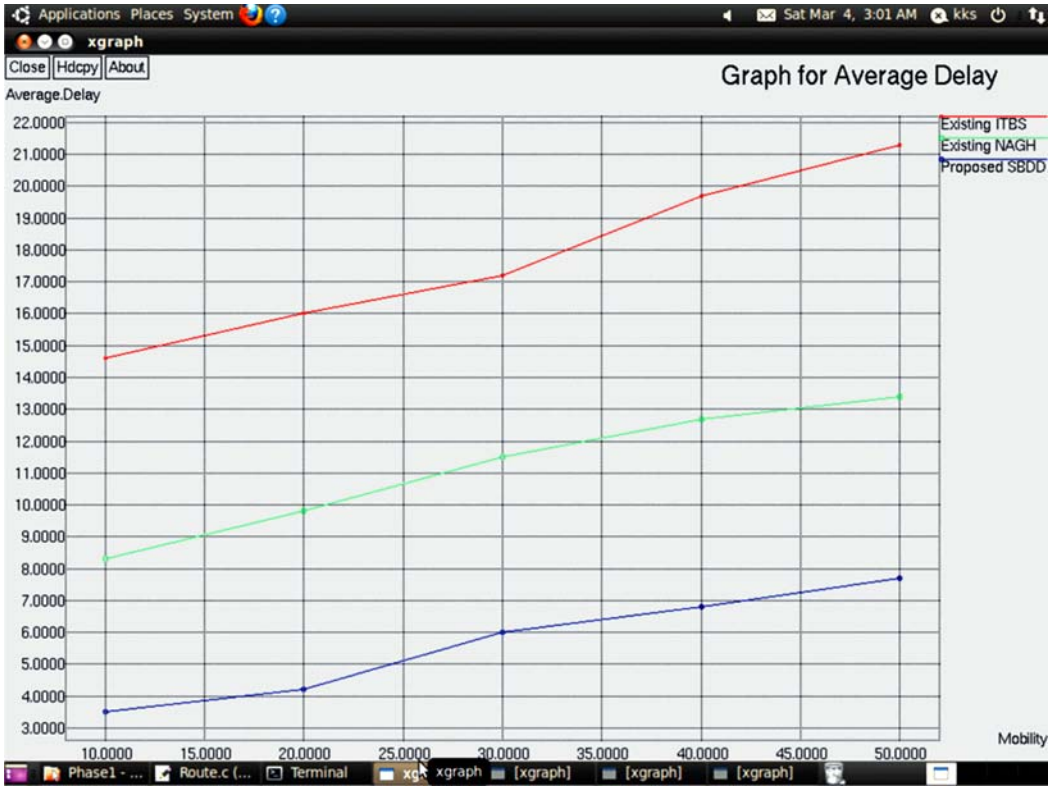

Figure 4: Graph for Nodes vs. Average Delay

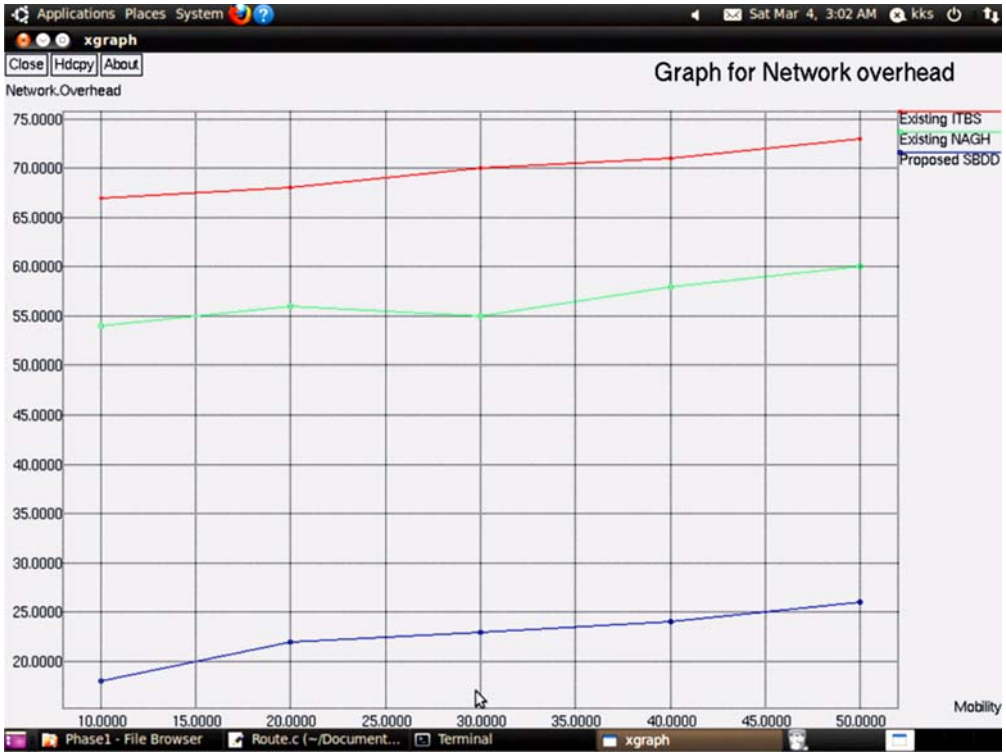

Figure 5: Graph for Pause Time vs. Network overhead

Average Throughput: Figure 6 shows Average throughput which is calculated by packet received degree from packet sent degree in certain speed. Usually node speed is fixed in sensor network; simulation rate is set to 100, heavily covered and stitched packets only allowed for transmission. In proposed SBDD scheme average throughput is raised compared to existing methods ITBS and NAGH.

Average Throughput = (Number of packet received/Sent)*speed

Figure 6: Graph for Nodes vs. Average Throughput

Network Lifetime: Figure 7 show that Lifetime of the network is predictable by complete process of network, resource utilized to done communication successfully. In proposed SBDD scheme Network Lifetime is improved compared to existing methods ITBS and NAGH.

Network Lifetime = length of energy usage/overall energy

Energy Consumption: Figure 8 shows consumption of energy; identified total energy utilized from starting node to ending node. In proposed SBDD scheme have enhanced packet transmission, it only forward original data packets in network, therefore energy consumption is minimized when compared to existing methods ITBS and NAGH.

Energy Consumption = Initial Energy-Final Energy

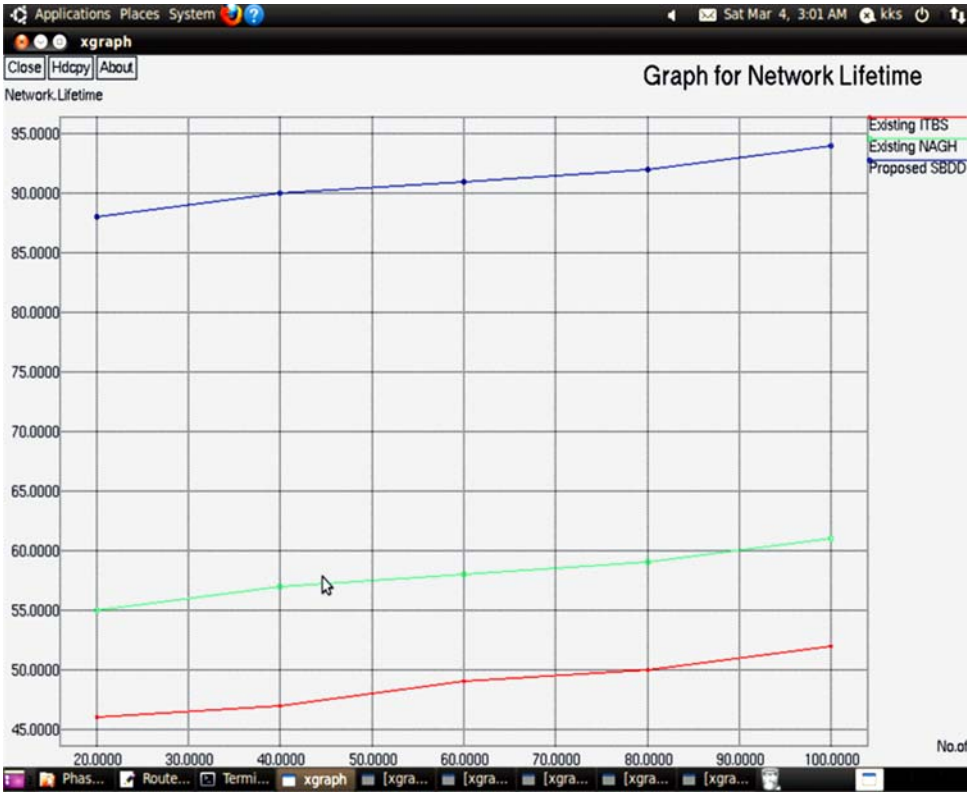

Figure 7: Graph for Nodes vs. Network Lifetime

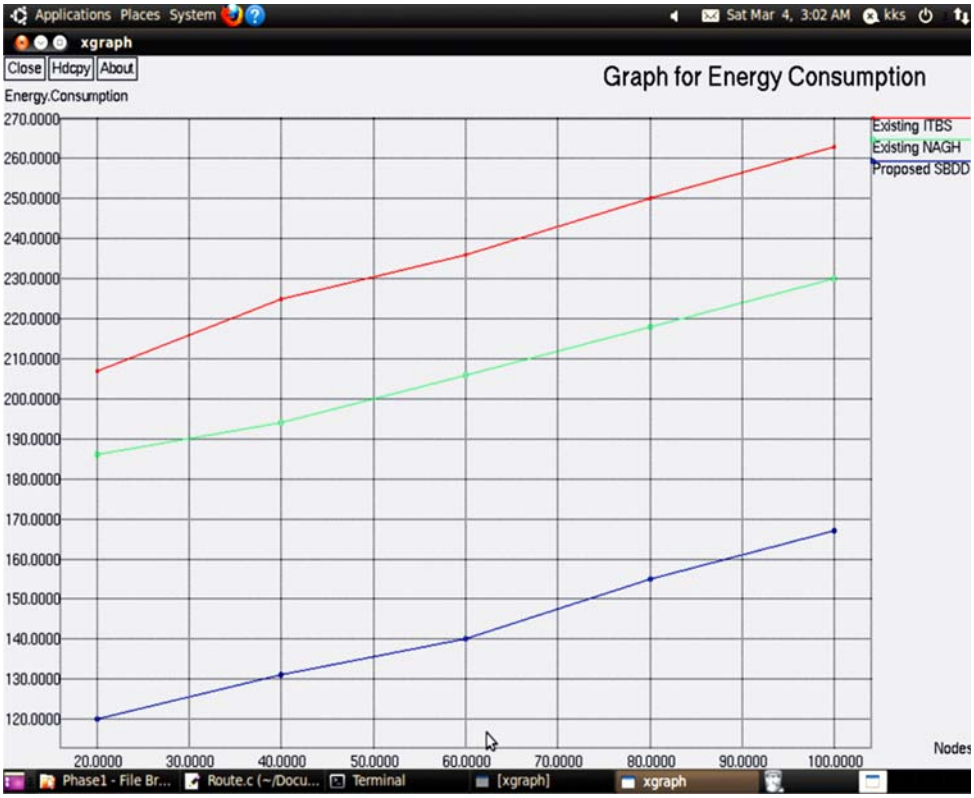

Figure 8: Graph for No. of Nodes vs. Energy Consumption

Packet loss: Figure 9 indicate that Packet losses are reduced since they are removing the duplicate data in the packet and send the correct original data during communication. Hence in the proposed SBDD scheme Packet loss is minimized compared to existing methods ITBS and NAGH.

$$\text{Packet Loss} = \left(\text{Number of packet}\frac{\text{Dropped}}{\text{Sent}}\right)*100$$

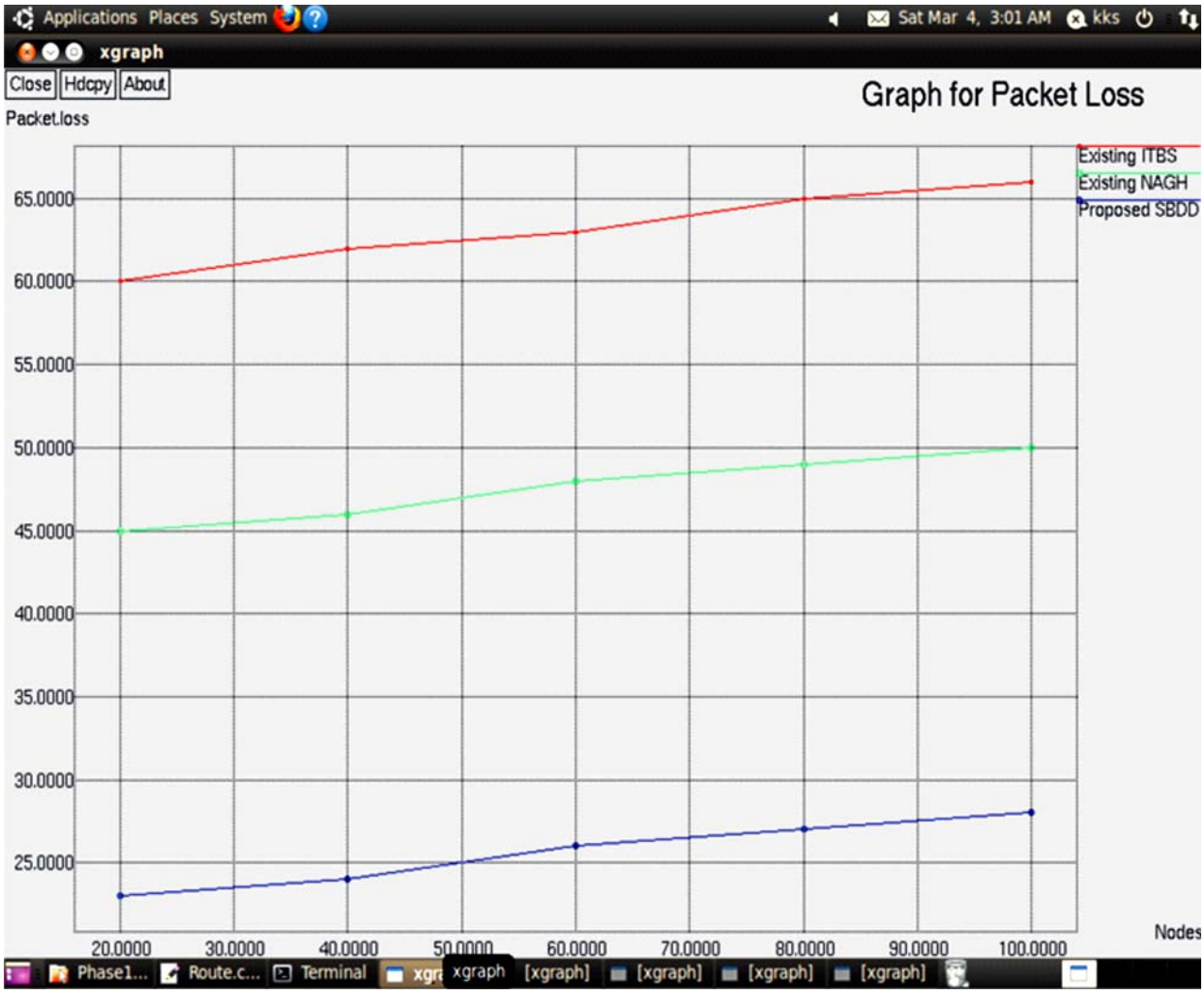

Figure 9: Graph for Node vs. Packet loss

5. CONCLUSION

In MANET, secure transmission is regarded as the most predominant feature. The MANET attempts to permit transmission across networks in which the topology and membership can varies often. Their typical characteristic is that nodes in the network require working with their peers in maintaining the network functionality. In such a case, intruder nodes can inject the duplicate data and try to retrieve the original data during the data transmission. The intruder node can make use of original data for data communication. Due to this, in network there is lot of fake data that affects the normal flow of data and deteriorates the performance of the network. Proposed Security Based Duplicate Data removing technique (SBDD), improves packet transmission. The proposed scheme identifies the incorrect duplicate data from the data packet and separates it before transmitting the

data. Data dribbling algorithm is utilized that helps to filter the fake information. This scheme is implemented in every node present in the routing route and finds the intruded data packets easily and at last it transmits the original data to the destination node. The proposed method supports the transmission with free of intrusion. Thus it minimizes the packet loss. It enhances the rate of throughput and lifetime of network. In future, this can be concentrate on improving the path stability and to acquire the effective transmission in the presence of various attacks.

REFERENCES

[1] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[2] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." IEEE wireless communications 11, no. 1 (2004): 38-47.

[3] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[4] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T.Imielinski and H. Korth, Ed., Kluwer, 1996.

[5] IEEE Std. 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications," 1997.

[6] B. Schneier, Secret and Lies, Digital Security in a Networked World, Wiley, 2000.

[7] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," ACM MOBICOM, 2002.

[8] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," ACM WiSe, 2002.

[9] Gopalakrishnan, S. and Ganeshkumar, P. 2014. Intrusion detection in mobile Adhoc Network using secure routing for attacker identification protocol. American Journal of Applied Sciences 11(8), 1391-1397.

[10] Muktikanta Sa, and Amiya Kumar Rath 2011. A Simple Agent Based Model for Detecting Abnormal Event Patterns in Distributed Wireless Sensor Networks. Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, 67-70.

[11] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture," IEEE 2011.

[12] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho 2012. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9(2).

[13] Bo Sun, Xuemei Shan, Kui Wu, and Yang Xiao 2013. Anomaly Detection Based Secure InNetwork Aggregation for Wireless Sensor Networks. IEEE Systems Journal, 7(1).

[14] Chang, J.M., Tsou, P.C., Woungang, I., Chao,H.C., and Lai, C.F. 2015. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach.IEEE Systems Journal, 9(1).

[15] Renyong Wu, Xue Deng, Rongxing Lu, and Xuemin (Sherman) Shen 2015. Trust-Based Anomaly Detection in Emerging Sensor Networks. International Journal of Distributed Sensor Networks. 2015(363569), 1-14.

[16] Haripriya, Y., Bindu Pavani, K.V., Lavanya, S., and Madhu Viswanatham, V., "A Framework for detecting Malicious Nodes in Mobile Adhoc Network," Indian Journal of Science and Technology, vol. 8, no. S2, pp. 151–155, 2015.

[17] Nanaware, Pradnya M., and Sachin D. Babar. "Trust system based intrusion detection in mobile ad-hoc network (MANET)." Next Generation Intelligent Systems (ICNGIS), International Conference on. IEEE, 2016.

[18] Lupia, Andrea, and Floriano De Rango. "Trust management using probabilistic energy-aware monitoring for intrusion detection in mobile ad-hoc networks." Wireless Telecommunications Symposium (WTS), 2016. IEEE, 2016.

[19] Nguyen, Dang Quan, Mylène Toulgoat, and Louise Lamont. "Impact of trust-based security association and mobility on the delay metric in MANET." Journal of Communications and Networks 18.1 (2016): 105-111.

[20] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks." Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012.