Advances in Modelling and Analysis B
Vol. 61, No. 3, September, 2018, pp. 151-157
Journal homepage:http://iieta.org/Journals/AMA/AMA_B

# Reducing packet dropping attacks in Manets using auditor and one hop approach

Lankapalli V. Ramesh[1]*, Chettiar R. Bharathi[2]

[1] Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu. &Assoc. Prof., Andhra Loyola Institute of Engineering and Technology, Vijayawada-520008, Andhra Pradesh, India
[2] Department of ECE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu 600054, India

Corresponding Author Email: rameshloyolacse@gmail.com

https://doi.org/10.18280/ama_b.610308

**Received:** 2 July 2018
**Accepted:** 25 August 2018

***Keywords:***
*manet, detection, delivery ratio, one hop, auditor, prevention,watchdog*

## ABSTRACT

Mobile Ad hoc Network (MANET) is an autonomous, wireless network of mobile devices with dynamic infrastructure. Despite its wide-ranging applications, MANETs are prone to network attacks eventually leading to denial of service attack resulting in packet loss. Blame it on the basic routing protocols such is their design assuming there are no malicious nodes in the network making them vulnerable to either black hole or gray hole attacks. Detection and elimination of malicious nodes involved in the packet forwarding process, is quite a challenge. Down the ages different methods have been employed for the same such as the credit based, trust based, auditing based and end to end based each having its own drawbacks. Aimed at improving the delivery ratio of packets in the network, the proposed method combines one hop with auditor for attack prevention and detection and watchdog mechanism can be combined with auditor node which identifies malicious nodes, so that there is a high level of security in adhoc networks. By taking an extra hop of traversal a situation is created where the malicious nodes tend to drop its own packets while the auditor tries to key out nodes which are malicious leading to its subsequent elimination.

## 1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a wireless network for communication among mobile devices. Routing protocols in MANET are been classified into reactive and proactive routing protocols. One most important characteristic of MANET is that they can form a network when needed at ease without any centralized node for controlling the different nodes that are present in the network. Each of these nodes can act as both router and host. Network is maintained by the individual nodes present. The mobile nodes present in the network is very limited to the range each nodes can transfer the information, so one or more nodes are needed in the successful delivery of the packet to the destination, therefore packets usually take multiple hops. The nodes between the sender and receiver are normally called as the intermediate nodes. These intermediate nodes act as a router in the packet forwarding process between the sender and the receiver. As there are much advancements in the field of MANETs, they are been used in different areas because of their ease of implementation, but they are also vulnerable to many attacks. The vulnerability was mainly due to the design method in the popular MANET protocols like Ad hoc on-demand distance vector

(AODV) [1] protocol and the dynamic source routing (DSR) [2] protocol. Both these protocols are designed in such a way that, it assumes that there are no malicious nodes in the network and routing takes place considering all the nodes as normal nodes even when there are malicious nodes in the network. This packet dropping attack exploit the shortest route concept in the packet forwarding process and advertise itself having the shortest path to the destination and drops the packet.

Over the years, different routing protocols have emerged. Some of the methods include the trust based, end to end acknowledgment based, credit based and auditing based methods. Each of the method uses different techniques and methods for detecting the malicious node. The maliciously identified nodes are eliminated from the network after detection.

These above methods perform fair in the detection and elimination of malicious node from the network from further forwarding of packets through the malicious node when comparing with the basic AODV and DSR protocols. Even though the existing methods are capable of detecting the malicious nodes and eliminating those nodes, these methods are not capable in the preventing the malicious nodes from the network. This work aims the prevention of the packet dropping attack. The prevention of malicious attack is carried out by taking an extra one hop in the packet forwarding process when the malicious node launch a cooperative attack in the network and an auditor method is combined with the one hop method to detect the single malicious attacks. The advantage of the proposed method is that the malicious nodes may suffer from dropping its own packets and thus forcing the malicious nodes to take participate in the packet forwarding process together with the detection of malicious nodes. This can eventually lead to the depleted number of malicious nodes present in the network when comparing with the existing protocols. This method therefore focuses on increasing the delivery ratio.

The analysis of the work is carried out in the ONE simulator [3]. One simulator uses different movement models for generating the node movement. Mobility and message passing can be visualized real time using its graphical user interface.

Delivery ratio of the proposed method is analyzed using the ONE simulator. The post processing tools used in ONE simulator helps in the evaluation of experiments and emulation of the real world DT N. The rest of the paper is organized into four sections. Section II discusses the related works. Methodology is discussed in section III. Section IV involves the analysis of the work and the conclusion of the work is given in section V.

## 2. RELATED WORKS

This section discusses the attacks, existing detection methods and simulation.

### 2.1 Attacks

Networks are subjected to different types of attacks. Passive attack includes traffic analysis and password capturing etc. An active attack comprises the activities such as modification, fabrication and dropping of data whereas the Denial of service attacks involves the misuse of the services. Packet dropping attack is a form of denial of service attack. Packet dropping attack results in the dropping of packets between the sender and the receiver. These attacks can however disturb the operations of a network and can reduce the performance of the entire network eventually. Multiple paths exist between the sender and receiver and the sending node broadcast request for shortest path to the destination. If the neighboring node has information regarding the path [4], it replies back the information of the path back to the sender. The route request packet is termed as RREQ and route reply packet is often termed as RREP. There can be chance that the first neighboring node to the sender may not have any information regarding the path, so the only action the neighboring node can do is the forwarding of these request packet to the very next neighboring node.

This process continues until a valid path is found between the sender and the receiver. The acknowledgment is received back along the reverse path when a packet successfully reaches the destination. The malicious nodes exploit this advertising strategy of route request of the sender node to launch packet dropping attacks. Normally in the case of packet forwarding process, once a valid path is established between the sender and the receiver, each intermediate node forward the packets coming through and the packets are delivered successfully to the destination. But in case of malicious nodes, it first advertises or replies to the sending node that it has the shortest path to the destination and that request initiates the packet forwarding process through that particular malicious node. But the malicious node actually agrees on forwarding and does the dropping of the forwarded packets. Packet dropping attack [5-6] is mainly of two types, that is the grey hole and black hole attack. The difference between the grey hole and the black hole attack is that the former is more of timely behavior attack while the latter is a continuous one.

### 2.2 Detection methods

The detection of packet dropping attack can be done by different methods that have been implemented over these years. Main methods include the trust based, credit based, end to end acknowledgment based and auditing based approaches. The first category is the credit based [7-8] systems. In this method, each node participating in the network is assigned with a counter called the credit counter and a security module. If a node wants to send data, the route is established, and then the security module counts the number of intermediate nodes between the sender and the receiver. The security module is a tamper resistant module.

If the credit of the sending node is greater than or equal to the number of intermediate nodes in between, it can send the data otherwise the node cannot send the data packets. If an intermediate node forwards the data packet, the credit counter for that intermediate node is increased by one. Here for the forwarding of the packets a security association established between the neighboring nodes. If this security association is not established, sending will not be successful. The credit counter for the sending node is not immediately increased, but the security module of the neighboring node increases the pending credit counter of the sending node. Thus security module of each node maintains a credit for all other neighboring nodes.

The second category is the end to end acknowledgment [9-12] based systems. Here an acknowledgment is been sent between consecutive neighbor nodes after sending one data packet. In the case of TWOACK method, an acknowledgment is been sent to the sending node when the send data packet reaches the third node or it travels two hops. Normally if nodes send out a data packet over two hops, the sending node is unable to know whether the consecutive or the next node to the consecutive node sends or drops the packet. The consecutive nodes may be packet dropping node. TWOACK method overcomes the problem by sending out an acknowledgment packet when the packet travels two hops. This two hop acknowledgment helps the sending node to know whether the consecutive nodes have sent the data packet or not.

When sending the data packet from the sending node to the neighboring node, neighboring node receives the packet and start forwarding the data packet to the very next node. Upon receiving the data packet at the node three, the third node extracts the routing information from the original data packet which has the routing information from the sending node to the third node. This routing information helps in determining the path for sending back the acknowledgment. The acknowledgment packet is been sent back to the second node and then to the sending node. A timeout period is been set for every node when an acknowledgment is been sent between the consecutive nodes. The same procedure is repeated in triplets until the packet is received at the destination node.

The third category is the trust based or the reputation based systems. Here in the trust based systems [13-19], each node participating in the network is assigned with a neighboring trust degree. Each node maintains a trust for each other neighboring nodes. When a node sends a data packet, the sender does not know whether the neighboring nodes or the intermediate nodes between the sender and the receiver will be forwarding the packets to the destination. When a packet arrives at a particular node, the current node updates the trust degree of the node which forwarded the packet and the node which forwarded the packet decreases the trust of the current node, as the forwarded node is unable to understand whether the current node is willing to forward the packet. Initially the trust degree is set as one which is the upper bound of the trust degree and lower bound of the trust degree is set to zero.

The trust degree increases or decreases based on the participation of each node in the packet forwarding process.

Based on the trust scheme, trust degree of the intermediate nodes receiving the packets is reduced even when it is a normal node. To issue this, when the packet reaches the destination, the path of the packet is extracted by the destination node and the destination node sends an acknowledgment back in the reverse path which stabilizes the trust degree of the normal nodes in the network.

The fourth category is the auditing based method [20]. Auditing based method employs the mechanism of trust based method along with the external mechanism called the auditor. Auditor is an external entity in the packet forwarding process. Auditor does not participate in the packet forwarding process. The external auditor analyzes each node for the malicious activity. The auditor requests each node to share the packet information to be shared with the auditor. Each node when requested gives the updated information to the auditor and if a node fails to share the information with the auditor, that particular node is classified in to the malicious category.

In the case of the end to end acknowledgment based scheme, the system is not able to find the correct node that is malicious. Coming in the case of trust based approach, considerable amount of packets are dropped when cooperative malicious attack is launched. In the case of credit systems, more number of malicious nodes may make some of the malicious node to be not detected while launching a selective packet dropping attack. When it comes to the auditing based method, delivery ratio is less. Some other methods [21] identify the number of malicious node present in the network by counting the number of packets delivered and created. These methods are able to detect and remove the malicious node from the network. But prevention of the packet dropping attack is not achieved with the above methods.

### 2.3 Simulation

Opportunistic Networking Environment (ONE) simulator is mainly developed for the simulation of the routing and application protocols. Different types of synthetic movement models and traces of real world scenarios by the user. It provides the framework for the routing. ONE engine is an agent based discrete event simulation. The simulation engine at each step updates the modules which performs the main simulation functions. The main functions of the ONE simulator includes the modeling of routing, message handling, node movements, inter-node contacts, post-processing, reports and visualization tools are used for the collection of result and the analysis.

Based on the number of packets delivered and the number of packets dropped. The malicious activity in the network is identified using this approach. But a drawback in this auditor approach is the lower delivery ratio. We are proposing an enhancement to this auditor approach for improving the delivery ratio of the network by introducing an extra one hop. One hop represents the path between two nodes. An extra one hop of traversal is implemented in the message delivery process along with the auditor method. We call the proposed approach as AOH method here after in this paper.

## 3. PROPOSED METHOD

The Architecture is illustrated in the Figure 1, here the nodes present in the network is categorized in to sender node, intermediate nodes, receiver node, and auditor. Many intermediate nodes are present in between the source and the destination. The sender node is represented as S and the receiver is represented as R. Intermediate nodes are represented as IN. The node which does not participate in the packet forwarding process is represented as N. The sender S takes the shortest path to the receiver R by choosing the intermediate nodes IN1, IN2 and IN3. An external auditor is also present in the network represented by A. The one hop traversal is represented in dotted lines. The main components of this architecture include the following;

Sender Node: Sender is the node which initializes the process of sending data to a destination. Route discovery and encryption is done at the sender side. When the sender S wants to send a message (msg) to the receiver R, route discovery phase is initiated by the sender node. The two processes in this phase are the route request and the route reply. All the nodes in the network distribute their public key with each other after route discovery. Each and every information is updated in the routing table. The node requires a key to perform encryption of data. The sender node use the public key of the destination and perform encryption of data.

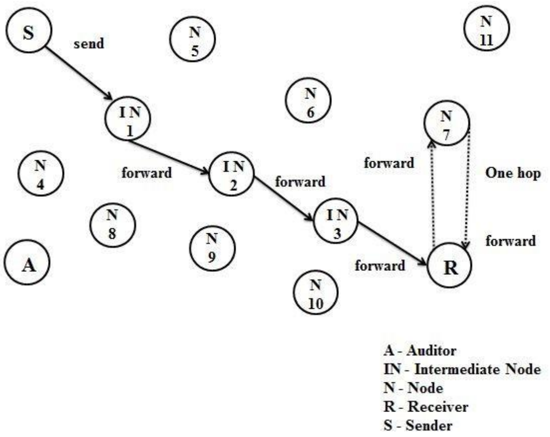


**Figure 1.** Architecture of manet with aoh

The node which wants to initiate transmission must register with the auditor node by providing all information of the Manet. The updated routing table information is monitored by the Auditor Node. The sender node will create a key for each and every intermediate node and send the key to them and also to the Auditor node for performing validation of intermediate nodes. Now data transfer is initiated. When the data is encrypted by the public key of the destination based on routing table information the data transfer will proceed. The algorithm used for performing crypto method is

For Encryption $C = M^e \bmod n$

For Decryption $M = C^d \bmod n = (M^e)^d \bmod n = (M)^{ed} \bmod n$

**Algorithm**

- Choose two large prime numbers p and q
- Compute $n = p * q$
- Choose the public key e such that $\gcd(\phi(n), e) = 1; 1<e<\phi(n)$
- Select the private key d such that $d*e \bmod \phi(n)=1$
- Public key is (n, e) and Private key is (n,d)

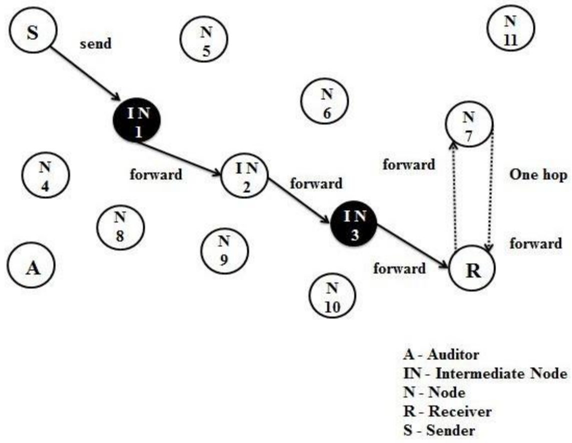


**Figure 2.** Attack model

Intermediate Nodes: At each intermediate node between the sender and the receiver, the node has to provide the key to the Auditor node provided by the sender node to perform validation of the node so that there is no chance of any miscellaneous action in the network.

When an intermediate node receives the data packet it has to provide the key to the Auditor node for validation. When the node is validated then only it can send data packets to its neighbor. This process continue until all intermediate nodes are validated.

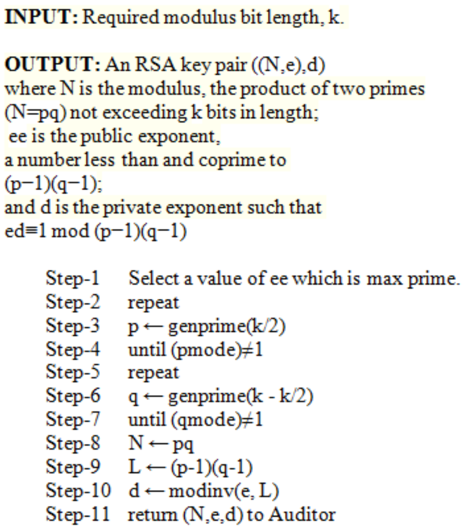
This process helps in avoiding malicious nodes entering into manet and also to avoid miscellaneous actions like packet drops, routing data modifications etc.

Receiver Node: Receiver node is the node which receives the data. When the node receives the information then the data packets are in encryption form. Now the receiver will send a request to the auditor asking for private key.The auditor will verify the validitiy of the node and generate the private key and send it to the receiver which is monitored by one hop node.Now the data can be decrypted.In this way successful transmission takes place

The key pairs are generated using the below algorithm.

Auditor Node: Auditor is an external entity who has no participation in the packet forwarding process. The main aim of the auditor is to collect information from the nodes that participate in the packet forwarding process and to check whether there is any malicious activity in the network. The auditor finds malicious activity based upon the routing information collected from the different nodes. The auditor holds the routing table of the manet which is provided by the registered node i,e sender node. When this node gets a request from the destination, it will generate the key and forwards to the destination which is monitored by one hop node. By maintaining Auditor node the data is secured. Along with the auditor node, watchdog mechanism is also used for monitoring the entire network. Watchdogs are outstanding amongst other systems to distinguish the dangers and assaults from the malicious nodes in the systems. The Watchdog is utilized to enhance throughput in a MANET, by recognizing making trouble node, which trap different nodes, by consenting to forward the packets without ever doing as such. While the watchdog is utilized to distinguish malicious nodes from normal ones the watchdog monitors all nodes in the network.

One Hop Node: The one hop node in the model is taken as node N7 which is an adjacent node to the receiver R. Each packet traverses through N7 before reaching receiver by taking an extra one hop.With this one hop destination node is monitored and the data will be received to one hop node before destination.The private key is only received to one hop node based on routing table information and then one hop node will moniter the key and data.If the destination sends request to the Auditor node for private key then the Auditor node will generate the key and send it to one hop node and then this one hop node will send the key to the destination.The destination then decrypts the data which is monitored by one hop node.By this unauthorized nodes which acts as destinations can be avoided in accessing sensitive data.



**INPUT:** Required modulus bit length, k.

**OUTPUT:** An RSA key pair ((N,e),d)
where N is the modulus, the product of two primes
(N=pq) not exceeding k bits in length;
ee is the public exponent,
a number less than and coprime to
(p−1)(q−1);
and d is the private exponent such that
ed≡1 mod (p−1)(q−1)

```
Step-1    Select a value of ee which is max prime.
Step-2    repeat
Step-3    p ← genprime(k/2)
Step-4    until (pmode)≠1
Step-5    repeat
Step-6    q ← genprime(k - k/2)
Step-7    until (qmode)≠1
Step-8    N ← pq
Step-9    L ← (p-1)(q-1)
Step-10   d ← modinv(e, L)
Step-11   return (N,e,d) to Auditor
```

## 4. PREVENTION & DETECTION MODEL

As the network is made up of nodes, it involves both the normal and the malicious nodes. The attack model is illustrated in the Figure 2. The intermediate nodes present between the source and destination can be either a malicious node or it can be a normal node. If the node is a malicious node, it initializes a packet dropping attack and drops the packet. The malicious nodes present in the path between source and destination can communicate each other and initialize a cooperative packet dropping attack.

For example the intermediates nodes IN1 (malicious node) and IN3 (malicious node) can launch a cooperative attack. The intermediate node IN1 triggers IN3 to drop the next incoming packets from the sender S. But in the packet forwarding process, the packet takes an extra hop of traversal to the one hop node N7. As the route information is encrypted, the receiver does not know that the packet is for itself when the packet reaches initially at the receiver R. R understands that the packet is for itself only when the packet reaches the R after taking one hop of traversal.

This one hop traversal of the message with encryption hides the fact from the intermediate malicious node IN3 that the message is for itself when intermediate malicious node IN1 triggers a cooperative attack to the IN3. This mode of traversal with encryption makes the malicious node unaware of the fact that the message is for itself or not and if it drops the message, the attack do not take place in the case of cooperative attack. Thus it creates a situation in which the malicious node can drop its own message. This forces some of the malicious nodes to take part in the packet forwarding process suppressing their malicious behavior. If there is a validation error at Ni, then Ni-1 is detected as malicious.

But with the above method, single malicious activity on the network cannot be reduced. Therefore an auditing based trust mechanism is used to identify the malicious behavior. The auditor requests the number of packets send and received at each node. Each node replies the information back to the auditor. The auditor compares the number of packets send and received. Success is the number of packets delivered and failure represents the number of packets dropped. Three conditions checked by the auditor are;

If success < failure at Ni, Ni is marked as malicious.

If success > 0, failure > 0 & success > failure at Ni, link break at Ni.

If failure = 0 at Ni, Ni is marked as normal.

With the above conditions, the auditor is able to identify the malicious and normal nodes along with link breaks and packet dropping.

In the normal method, the malicious node drops the messages and there is no mechanism for detecting these drops. In the case of the auditor method, the probability of detection of malicious nodes and removal is taken as 25% and is set as the overall delivery success in the network. The rest 75 % is set as the probability of unsuccessful delivery. This 75% is the probability of undetected malicious nodes and link errors.

The two state of behaviors used for simulating AOH method are B1 and B2. B1 represents the malicious packet dropping behavior of the malicious nodes while B2 represents the suppressed behavior of the malicious node. The aim of the one hop method implemented in the proposed method is to prevent the malicious node from dropping the packets. When using the one hop protocol, the malicious node does not know whether a packet is for itself or not thereby creating a situation for it to drop its own packets. Therefore some malicious nodes suppress the behavior and forward the packet. This suppressed behavior is taken as 25% of the successful delivery in the 75% of unsuccessful the delivery exhibited in the auditor method. AOH method therefore adds an extra percentage of success than the auditor method.

## 5. RESULTS AND DISCUSSION

The simulation was carried out in the NS2 simulator. A comparison has been drawn between the proposed and auditing methods. Based on the analysis, which focus on the delivery ratio of the packet, the results are graphically presented below.

Three methods were analyzed in the simulation. It includes;

Normal method

Auditor method

Auditor & One Hop (AOH) method

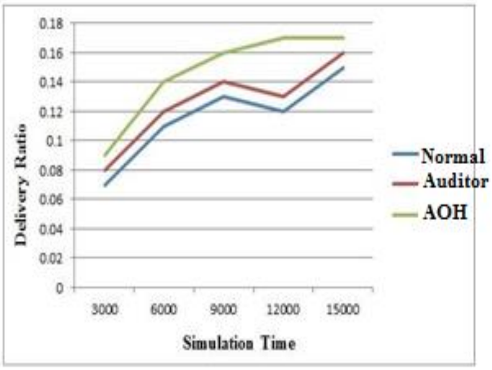


**Figure 3.** Delivery ratio: 10% malicious nodes

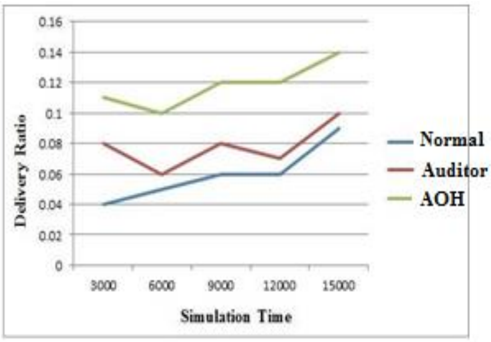


**Figure 4.** Delivery ratio: 20% malicious nodes

Delivery ratio is taken on the y axis and simulation time is taken on the x axis. The delivery ratio is the percentage of message delivered to that of message created and is calculated using the below equation.

$$\text{Delivery Ratio} = \frac{\text{no. of messages delivered}}{\text{no. of messages created}} \qquad (1)$$

The three methods are compared and illustrated in Figure 3 and Figure 4 with 10% and 20% malicious nodes respectively. The number of packet dropping increases with the increasing number of malicious nodes. However, the AOH method shows much better performance in delivery ratio than other methods.

The delay of data transmission between the nodes is reduced in the proposed AOH method and is illustrated in below figure.

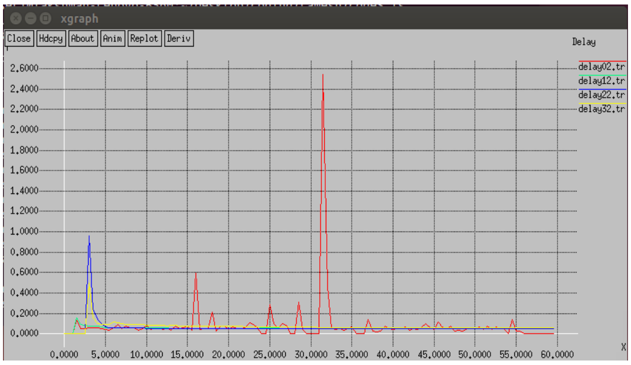


**Figure 5.** Delay in data transfer

The proposed method reduces the packet loss during communication. The auditor and one hop method effectively each node whether it has forwarded the packets to next nodes without any miscellaneous action. The packet loss reduction levels are depicted in below figure.

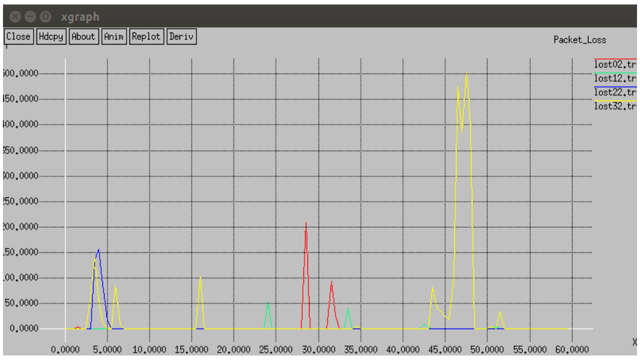


**Figure 6.** Packet loss reduction

The throughput of the proposed method is better than the existing methods. The results show that the proposed AOH method exhibits best and better performance than the traditional methodologies.

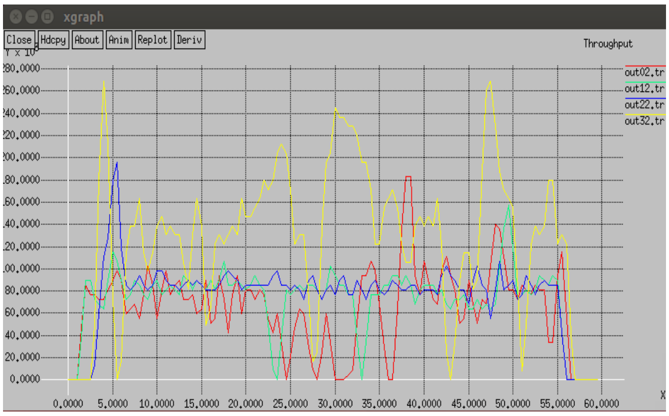


**Figure 7.** Throughput level

## 6. CONCLUSION

The lack of centralized infrastructure and the free motion of nodes in the network results in link errors. Since the basic MANET protocols are unable to detect the malic ious packet dropping; the network was vulnerable to packet dropping attacks by malicious nodes which possess a serious threat to the network. The malicious activity in the network was identified using different methods like trust based, credit based, end to end acknowledgment based and auditor based methods. Even with the existing packet dropping detection methods, the detection and elimination of the malicious nodes was less and thus resulting in the reduced delivery ratio.

The proposed method which uses the combination of auditor and one hop (AOH) approach was aimed at improving the delivery ratio of the network by preventing and detecting the malicious packet dropping. The one hop method helps in the prevention of the packet dropping attack while the auditor method helps in the detection of malicious packet dropping. This prevention and detection approach used in the proposed method helped in improving the packet delivery ratio of the network. As the number of malicious nodes in the network increase, the number of packets dropped also increase. But the AOH method showed better performance compared to other methods regarding the delivery ratio of the network.

But there remain issues to be explored for future studies. One hop method was used for preventing the cooperative malicious attacks and auditor method for detecting the single malicious attacks. The combination of auditor and one hop method adds an extra overhead for packet transmission. Thus there exists a need to develop a new routing mechanism for preventing and detecting cooperative and single malicious attacks using less overhead.

## REFERENCES

[1] Perkins C, Royer E. (1999). Ad hoc on-demand distance vector routing. In Proc. of IEEE Workshop on Mobile Computing Systems and Applications 90-100.

[2] Johnson D, Maltz DA, Broch J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In Ad Hoc Networking 139-172.

[3] Kernen J, Ott, Krkkinen T. (2009). The ONE simulator for DTN protocol evaluation. Simutools 09 Proceedings of the 2nd International Conference on Simulation Tools and Techniques.

[4] Perkins, Bhagwat P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proc. SIGCOMM 94: Computer Communications Review 234-244.

[5] Nakayama H, Kurosawa S, Jamalipour A. (2009). A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. IEEE Transactions on Vehicular Technology 5: 2471-2481.

[6] Sun B, Guan Y, Chen J, Pooch U. (2003). Detecting black hole attack in mobile ad hoc networks. IEEE Transactions on Vehicular Technology 490-495.

[7] Buttyan L, Hubaux JP. (2003). Stimulating cooperation in self organizing mobile ad hoc networks. ACM/Kluwer Mobile Netw. Appl 579-592.

[8] Zhong S, Chen J, Yang YR. (2003). Sprite: A simple cheat- proof, creditbased system for mobile ad-hoc networks. In Proc. IEEE INFOCOM Conf 1987- 1997.

[9] Balakrishnan K, Deng J, Varshney P. (2005). TWOACK: Preventing selfishness in mobile ad hoc networks. In Proc. IEEE Wireless Commun. Netw. Conf 2137-2142.

[10] Liu K, Deng J, Varshney P, Balakrishnan K. (2006). An acknowledgement based approach for the detection of routing misbehavior in MANETs". IEEE Trans. Mobile Comput 6: 536-550.

[11] Padmanabhan V, Simon DR. (2003). Secure traceroute to detect faulty or malicious routing. In Proc. ACM SIGCOMM Conf 7782.

[12] Papadimitratos P, Haas Z. (2003). Secure message transmission in mobile ad hoc networks. Ad Hoc Netw 1: 193-209.

[13] Bhalaji N, Shanmugam A. (2005). Dynamic trust based method to mitigate grayhole attack in mobile adhoc networks. International Conference on Communication Technology and System Design 881-888.

[14] MAOHmmad T, Kahvand M. (2014). Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks. 17th IEEE M editerranean Electrotechnical Conference, Beirut, Lebanon 13-16.

[15] Galuba W, Papadimitratos P, Poturalski M, Aberer K, Despotovic Z, Kellerer W. (2010). Castor: Scalable secure routing for ad hoc networks. In Proc. IEEE INFOCOM 1-9.

[16] Buchegger S, Boudec JY. (2002). Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks). In Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf pp. 226-236.

[17] He Q, Wu D, Khosla P. (2004). Sori: A secure and objective reputationbased incentive scheme for ad hoc networks, in Proc. IEEE Wireless Commun. Netw. Conf pp. 825-830.

[18] Liu Y, Yang YR. (2003). Reputation propagation and agreement in mobile ad-hoc networks. In Proc. IEEE WCNC Conf 1510-1515.

[19] Marti S, Giuli TG, Lai K, Baker M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proc. ACM MobiCom Conf, pp. 255-265.

[20] Shu T, Krunz M. (2015). Privacy preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. IEEE Transactions on Mobile Computing 4:

813-828.

[21] Shu T, Liu S, Krunz M. (2009). Secure data collection in wireless sensor networks using randomized dispersive routes. In Proc. IEEE INFOCOM Conf., pp. 2846–28508.