An Efficient Mechanism For Identification Of Malicious Node Of Wormhole In Dynamic Source Routing Protocol

Nisha Sharma, Manish Sharma, Durga Prasad Sharma

Abstract : The diverse characteristics of ad-hoc networks of being infrastructure-less, self-organized and spontaneous make the task more challenging to secure it. If a node needs to send data to a node that is beyond the transmission range of it, the sender node asks favor of other nodes in the network to reach the destination node. Thus the existence of the ad-hoc network is completely reliant on nodes cooperating and trusting each other. The repeated non-cooperative behavior of a node with other nodes makes it unreliable for future communication and is considered as a malicious node. However, this dependency of network nodes on each other makes MANET vulnerable to various kinds of security attacks. These security attacks can be categorized as Passive and Active attacks. Wormhole attack is an active attack and considered most dangerous as it can cause major damage to routing. Numerous secure routing protocols have been developed which are based on cryptography mechanism, need pre-organized structure, centralized authority, or need external hardware, etc. These mechanisms are impractical because of limited available resources in MANET. In this paper, we are proposing a novel trust-based mechanism on the concept of Node to Node packet delay for the detection of the malicious node in a wormhole attack. The trust value of each node is calculated by observing the packet transaction among adjacent nodes and based on this trust value identification of malicious node is carried out. The trust values can be further considered for making routing decisions and selecting a secured route.

Index Terms: MANET, DSR, Trust-Based, Wormhole Attack, NS3.

◆

1. Introduction

Mobile Ad-hoc Networks (MANET) became popular in a short period because of its indistinctive features of being infrastructure-less, spontaneous and use of license-free frequency band for communication between nodes. Nodes in MANET are self-organizing and work as host and router both [1]. These features make them attractive for significant applications such as Military communication, Automated battlefields, Search and Rescue operations, Policing and Fire Fighting, Virtual classrooms, Conference rooms, Sports Stadium and Library, Multiuser game, Outdoor internet access, etc. [2]. In MANETs nodes are mobile and topology is dynamic that makes Routing to be considered a big issue. The standard wired network routing protocol is impractical forAd-hoc routing. Numerous protocols for routing in MANET have been established over the past few years. In MANET, these protocols are divided into three ways proactive, reactive, and hybrid routing protocol. In Proactive Routing, every node in the networks maintains a table periodically which contains a route to reach all the other nodes. The route is available before it is needed which prevents latency delays of route discovery. Thus, it is also known as Table-Driven protocol. Whereas in Non-Table driven or Reactive routing protocol, the nodes in the network acquire or maintain routes only On-demand to preserve network resources. The hybrid routing protocol is blend of both Reactive and Proactive protocols. Increased use of Ad-hoc networks causing several security attacks and categorized into two types: Passive and Active attacks [3]. In an Active attack, a malicious node causes harm to network resources and may disturb routing information. Whereas in passive attack malicious node does not do any harm to network resources, its only intention is to extract information like network topology or node hierarchy. Once a malicious node gets involved in the discovered route for a transaction, it can launch many different kinds of activities like a drop, selective drop, message snooping, identity spoofing, etc. To stop these activities, it is needful to identify the malicious node and to develop secured routing in MANET. These attacks give a need to develop secured routing in MANET. Trust and security these terms are tightly bound when the secure system comes in the picture. The trust-based concept of Ad-hoc networks is based on the Human behavioral model, in which several people that are strangers to each other, need to communicate with each other having mutual trust in each other. Over some time, the trust gets more clarity. In this paper, we are proposing a mechanism in which the calculation of trust value of each node is performed by observing Node to Node (N2N) packet delay during the packet transaction among adjacent nodes and based on this trust value identification of malicious node is carried out. The trust values can be further used for making routing decisions and selecting a secured route. In this paper, we will be usiing DSR routing protocol for performance evaluation of the network in existence of malicious node. The organization of the paper is as follows, Section 2 discusses the previously proposed security solutions for MANET. Section 3 explains wormhole attack in Dynamic Routing Protocol. Section 4

- *Correspondence Author - Nisha Sharma, Research Scholar, SGVU, Jaipur, Rajasthan, India , E-mail : Sharma_nisha2005@rediffmail.com.*
- *Dr. Manish Sharma, Professor, HOD, CSIT, SGVU, Jaipur, Rajasthan, India.*
- *Dr. D.P. Sharma, Professor, MSRDC-MAISM, Jaipur, Rajasthan, India.*

gives a detailed description of the proposed mechanism. Section 5 explains the Extension of DSR. This section includes a brief explanation working of the proposed mechanism with DSR routing protocol. Section 6 is about the simulation of a wormhole attack in DSR protocol using NS3 environment and analysis of the result.

2. RELATED WORK

Several mechanisms have been evolved to prevent or detect malicious nodes in mobile ad-hoc networks. Some of the mechanisms are discussed briefly in this section. Hu et al. [4] Proposed a mechanism which is based on packet leashes and a protocol named TIK to implement these leashes. In this mechanism, the packet carries information within itself to limit the allowed transmission distance and avoid tunneling of the packet. The packet leash can be of two types: temporal and geographical leashes. In geographical leashes, neighbor relation is evaluated from the information of geographical location of node and protected synchronized clock. Whereas in temporal leashes, the allowed distance of a packet for transmission is evaluated by speed of light and signal propagation time. Geographical leashes do not need to have tightly synchronized clock that make them more beneficial over temporal leashes. It has the limitations of GPS technology. Capkun et al. [5] In this technique, to estimate the distance between 2 nodes Mutual Authentication with Distance-bounding (MAD) protocol has been used.It is based on the assumption that a transceiver is attached with every node as extra Hardware. It intake single bit and performs a 2-bit XOR over it. The result is then broadcasted. This mechanism, due to their efficiency and simplicity, is compliant with the limited resources of most mobile devices. It is likewise ready to adjust the conventions to the specific needs of a given application. The overhead is quite rational, and the mechanism is strong enough considering the attackers of various degrees of strength. This paper is solution for securing topology problems and encounter tracking; but prevention of the wormhole attack. Hu and Evan et al. [6] is based on directional antennas for finding and preventing the wormhole attack. Sharing of the directional facts is done between source and destination to evaluate the arrival of angle and direction of received signal. The mechanism is based on the concept that two communicating nodes receive signals at the opposite angles and assume that nodes uphold the correct sets of their adjacent nodes. This mechanism fails only when attacker form wormholes in the middle of two directional antennas. Khalil et al. [7] developed a Secure Neighbor Discovery and Monitoring Based approach called LITEWORP: Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Network. A central authority traces the location of each node in the network and separates the malicious nodes globally. In LiteWorp, nodes acquire full two-hop routing information from their neighbors. After authentication, nodes do not accept messages from those they did not originally register as neighbors. In LiteWorp nodes verify that all packets are forwarded properly as well as also confirm that no node is sending packets it did not receive. Since the node’s neighbors are determined and detected only once in LiteWorp, and the packets from non-neighboring nodes are rejected, no node movement is allowable. Therefore, LiteWorp applies to static networks only. As the network mobility increases the detection rate of this technique decreases. Jacob et al [8] Deployed mechanism named TrueLink which is a time-based concept. TrueLink confirms whether a node is directly connected with its adjacent neighbor or not. There are 2 phases involved in this technique: rendezvous and validation. In the first part nonce is exchanged between two nodes with a firm timing factor. In the second phase, the authentication check is performed on these two nodes for the original source of the corresponding nonce. Later, to avoid extra hardware include round trip time (RTT) approach. The RTT must be calculated by nodes between two adjacent nodes. This method is based on the concept that a genuine node has a lower RTT value than the malicious nodes. This technique works only for hidden attacks. Tran et al. [9] Proposed Transmission Time-based Mechanism (TTM). The mechanism is based on the concept of calculating transmission time between adjacent nodes along the recognized path. Detection of the wormhole is performed during the route setup procedure considering the fact that transmission time between two malicious nodes is much more than that transmission time between two genuine neighbors. There is special hardware required and performs less overhead of calculation. The limitation of this scheme is that it is explicitly designed for Ad Hoc On-Demand Vector Routing Protocol (AODV) only. Saurabh et al. [10] Proposed a mechanism based on Hound Packets. The source node starts the process of detecting wormhole in the recognized path. In it, the hop difference between the neighbors of the one-hop away nodes in the route is counted. In this method there is no need of any special hardware or accurately synchronized clock for detecting wormhole attacks and the protocol is also independent of the physical medium of the wireless network and also efficient in detecting wormhole of large tunnel lengths[10]. Dhruvi et al. [11] The author designed an identity-based signature mechanism along with clusters. Cluster head of Cluster-based architecture is selected in way that they cannot be malicious. The mechanism works in three phases namely the Setup phase, the Communication phase, and the secure data transfer phase. This scheme does not need to distribute any certificate among nodes, so it reduces computation overhead. Using this scheme performance of network improves in terms of throughput, packet delivery ratio, and end-to-end delay. The drawback of this technique is it protects wormhole attack that is launched by packet replay only. Sayan et al. [12] proposed Absolute Deviation Covariance and Absolute Deviation Correlation algorithms to detect Wormhole in MANET. The Correlation coefficient between packet sent and packet received is calculated to identify wormhole. If the correlation coefficient is high, the node is considered malicious. Further, the Absolute Deviation Correlation Coefficient is utilized to identify the wormholes by measuring the packet drop pattern. The proposed algorithm does not require any extra conditions for its execution; also it is lightweight and robust. The disadvantage of this method is it increases computational complexity and it also requires additional information to be known prior. Kavitha et al. [13] proposed a mechanism that works in 3 steps: Trust calculation,Trust-based routing and Key Generation. Trust is calculated based on the four different trust components such as affinity, trustworthiness, energy, and bandwidth. The nodes are classified as trusted or untrusted based on the calculated trust value and trusted nodes are qualified for a routing path. The Key Generation is based on the Diffie-Hellman key exchange method. The drawback of the trust-based mechanism is that it is time-consuming and need a lot of memory to store the required information for trust calculation. However, the false information may lead to calculate false trust value.

3. Wormhole Attack In Dynamic Source Routing Protocol

Dynamic Source Routing discovers the route only on demand when a node request for a route to another node with which it want to communicate. It is a source routing protocol where the source node provides the whole path that packet should traverse. However, it does not send any control traffic when there is no data transmission. A wormhole attack can be take place in DSR protocol by tunneling each RREQ packet straight to the destination target node of the RREQ. When neighbor of the destination node's hear this RREQ packet, they follow usual routing procedure to rebroadcast the RREQ and then discard all the other RREQ packets which are having same request ID, without processing . In DSR all the duplicate Route Request gets deleted if it has already been processed by the node previously, the malicious nodes take advantage of it and prevent any route from being discovered, other than through the wormhole. If the attacker is close to the source node, the routes containing more than two hops are prevented from being identified. The attacker then exploits the wormhole by dumping the data packets instead of forwarding, thereby creating a permanent Denial-of-Service attack or selective forwarding, modifying selective packets [4].

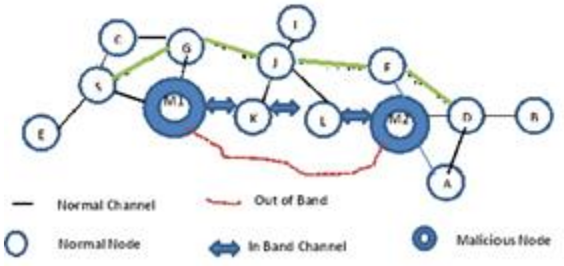


***Fig. 1**: Wormhole Attack In DSR*

As shown in Fig. 1 M1 and M2 are malicious nodes and establish tunnel between them as if they were one-hop neighbors. In a wormhole attack, these malicious nodes attract all the traffic towards the tunnel giving the illusion of having a shorter route them.

4. PROPOSED MECHANISM

The proposed technique is designed for the identification of malicious nodes in wormhole attack in MANET. Our trust-based mechanism is based on the concept of N2N packet delay. The trust value of each node is calculated by observing the packet transaction between nodes. This mechanism basically carried out in 4 steps: Finding neighbors, Calculating N2N trust value, Calculating aggregated trust value, and identifying malicious nodes. Every node in the network has to maintain a Trust Table as shown in Table 1: Trust Table. The node creating the Trust Table is considered to be a head node and the nodes which are directly connected to the head node are considered neighboring nodes. Each instance in the trust table is considered as trust entry and includes 3 attributes:

- Address of neighboring node.
- N2N Trust Value.
- PML is a list of Packet Metadata. Packet Metadata is an object with 2 attributes i.e. ID of Packet received by a head node from neighboring node and the time stamp.

Here the time stamp of every packet is important as the mechanism is based on the concept of delay between packets received by a head node from neighbor node (N2N packet delay).

Neighbor ID	N2N Trust Value	PML
<IP Address>	<Node to Node Trust Value>	{<Packet Meta List>}

***Table 1:** Trust Table*

The trust manager is responsible for calculating trust value periodically after a specified amount of time. The Trust Manager maintains and updates the list of PML against every neighboring node until the identification process is done and resets it after that. This mechanism basically carried out in 4 steps: Finding neighbors,

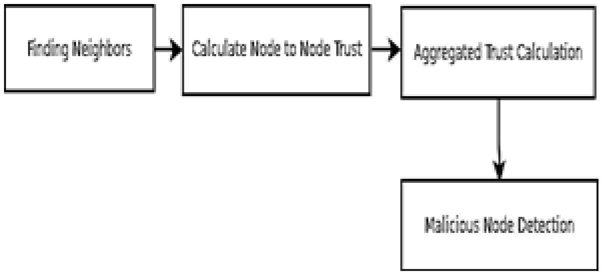


***Fig. 2:** Block diagram of Node to Node Trust based mechanism*

Calculating N2N trust value, Calculating aggregated trust value and identifying malicious nodes. Fig.2 represents the block diagram for identification of malicious node using the proposed mechanism:

4.1 Finding Neighboring Node

In DSR protocol, whenever a source node or any intermediate node broadcasts a route request (RREQ) to neighboring nodes that is in transmission range of it and every neighboring node who is receiving the route request (RREQ) will store the address of the requester (sender node) in the first column of its trust table. Considering every node as a head node and find the neighbors of each head node to create Trust Table entry.

4.2 Calculate N2N Trust Value

Calculation of the N2N Trust of every neighboring node is based on the collected information in PML. The value of N2N Trust varies from 0 to 1. High value (1) of N2N Trust denotes the most trusted node and low value (0) denotes less trusted. In ad- hoc networks the trust changes continuously due to the mobility of the nodes. Trust level cannot be represented clearly in discrete form as presence or absence of security, so we use continuous trend from complete distrust to complete trust.

Algorithm to calculate N2N Trust value

1. Initialize PEAK DELAY = 1.1 , Npeaks =0
2. Find size of PML (size)
3. Pic (Packet interval count) =size -1
4. Calculate packet interval for all the adjacent packet

   $$Pi = T_{(i)} - T_{(i-1)}$$

   Where
   Pi = Packet interval
   Ti = Timestamp of ith packet
   T(i-1) = Timestamp of (i-1)th packet

5. Calculate the average time interval between packets.

   $$S = \sum_{i=1}^{Pic} Pi \Big/ Pic$$

6. Calculate Peak Counts (Npeaks).

   FOR i IN 1 TO Pic
   $$Pi = T_i - T_{i-1}$$

7. IF Pi > S*PEAKDELAY THEN
   Npeaks= Npeaks +1
   END IF
   END FOR

8. Calculate current trust value

   $$CURRENTTRUST = 1 - Npeaks \,/\, Pic$$

9. IF $CURRENTTRUST \neq 1$ THEN

   N2NTRUST=(N2NTRUST+CURRENTTRUST)/2

   ELSE
   N2NTRUST = CURRENTTRUST

a. Calculate Aggregated Trust :

After step 2, we have a list of IP addresses of nodes and a list of N2N Trust values against each IP address. A single value of the N2N Trust value in the list means the node is recommended by only 1 neighbor node. Multiple values in the list means the node is recommended by multiple neighbors. The aggregated trust value of a node is required to calculate for those nodes having multiple trust values.

First, calculate the mean trust of each node (each IP Address) using the following formula.

1. Mean Trust Value:

   $$\mathrm{Tm} = \sum_{i-1}^{N} \mathrm{Tvi} \Big/ N$$

   Where ,
   Tm - Mean value of trust
   N - Count of N2N Trust value in list.
   Tvi - Trust value of ith recommendee.

2. Aggregated Trust value:

   $$Ta = Tm - \left(\frac{1}{Nt}\right) * (N-1)$$

   Where,
   Ta - Aggregated Trust value of node.
   Nt - Total nodes in the network or the maximum capacity of the network.
   N - Number of N2N Trust value in the list against the node (IP Address) or count of recommendee.

b. Identification of malicious node in wormhole attack:

At the end of step 3, we have trust values for all the nodes against their IP address in the Trust Table. The trust value is normalized between 0 and 1. The node having trust value 1, considered to be a most trustworthy node and trust value 0 will be considered as a most untrusted node. The obtained trust value can be used for making routing decisions. The node having a trust value near 0 must be avoided for further transactions. Now we have a list of untrusted nodes (IP Addresses) with their trust value but it is important to identify the malicious node from the list of untrusted nodes. To identify malicious nodes, we match untrusted nodes with the intermediate nodes of the discovered route in sequence. This sequence of the nodes represents the presence of wormhole. The DSR protocol can be augmented with the proposed node to node trust-based mechanism for finding the most trustworthy route.

5. EXTENSION TO DSR

When a node wants to send some packet to another node, the Source node first look for the route in its Route Cache, to the particular destination. If the route is not available then broadcast RREQ packet to neighboring nodes. Each intermediate node appends their IP address in the RREQ packet and keeps broadcasting the RREQ to its neighboring node until it reaches to the final destination. Duplicate RREQ packets are deleted by intermediate nodes. Every neighboring node who is receiving the RREQ creates a Trust Table and makes an entry of IP address of the sender node. The RREQ packet reaches to the destination contains the complete path from source through destination. Then the destination node sends an RREP packet containing the reversed complete path to the source node. The source node may receive more than one RREP having different routes. The source node can select any route considering a number of hops or delays or any other criteria. The Source node starts sending packets to the destination node using the selected route. The trust manager calculates and updates the trust value of the intermediate node by executing the proposed N2N trust-based algorithm periodically. As a final result, we have a list of IP address of the node and obtained trust value can be used for making routing decisions. The node having a trust value near 0 must be avoided for further transactions. The DSR protocol can be augmented with the proposed N2N trust-based mechanism for finding the most trustworthy route.

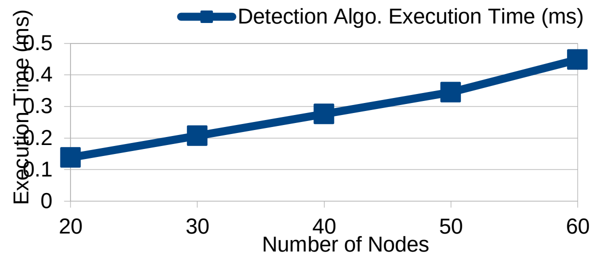
6. SIMULATION AND RESULTS

In this section, we present the simulation performance results of the N2N trust-based mechanism. We implemented and tested the mechanism using the NS-3 simulator. The experiments are conducted in the conditions that imitate actual deployment. The performance examination of the N2N trust-based mechanism is done using the DSR protocol and its implementation in NS-3[14][16]. As shown the Table II and Table III. Random Waypoint is chosen as a mobility model because it provides high flexibility for creating an ad-hoc network and also provides controlled access to the user for setting speed parameter. The metrics defined for interpreting the correct results from the simulation are the time taken to execute the proposed algorithm and detect malicious node. Time taken to detect a malicious node is considered after route discovery. We have applied different simulation scenarios to evaluate the performance of the proposed mechanism. We have taken 2 scenarios: In the first scenario, we are analyzing the execution time taken by the proposed algorithm by varying numbers of nodes in the network with fixed CBR value. The numbers of nodes taken for the experiment are 20,30,40,50 and 60 as shown in Fig. 3. From the results, it is clear that execution time increases gradually as the number of nodes increases but the maximum execution time of the algorithm is 0.45 ms which is a very negligible time value, this time value indicates the faster performance of the algorithm. As a final result, we have a list of untrusted nodes (IP Addresses) with their trust value. To identify malicious nodes, we match untrusted nodes with the intermediate nodes of the discovered route in sequence. This sequence of the node represents that the untrusted node belongs to the wormhole.

Table II: *Simulation Parameters of the 1st scenario*

Parameters	Values
Protocol	DSR
Simulation Time	30 Seconds
Simulation Area	1000m x 1000m
Number of Nodes	20/30/40/50/60
Transmission Range	250
Movement Model	Random Way Point Model
Maximum Node Speed	3 m/sec
Traffic Type	CBR (UDP)
No. of Wormholes	1
Malicious Nodes	2
CBR (Kbps)	64
Packet Size	512 bytes

Fig 3: Detection Algorithm Execution Time Performance Number of Nodes Vs Execution Time

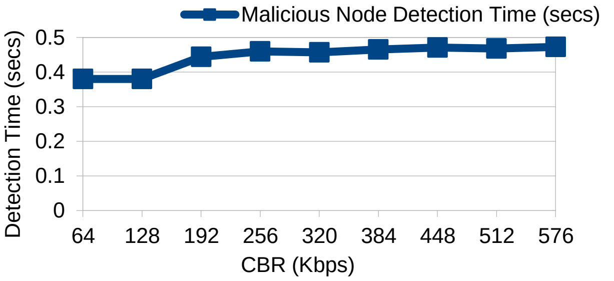


In the second scenario, we are analyzing the time taken by the proposed algorithm to detect malicious node by varying the value of CBR. The number of nodes in the network is 50 and remains unchanged. CBR value is varying from 64 to 576. As shown in the Fig. 4, CBR value is changing as 64,128,192,256,320,384,448,512 and 576. From the result, it is clear that the maximum time taken to detect the malicious node for a size of 50 nodes in the network is 0.472 sec which is negligible time and it remains constant for different values of CBR.

Table III: *Simulation Parameters of the 2nd scenario*

Parameters	Values
Protocol	DSR
Simulation Time	30 Seconds
Simulation Area	1200m x 1200m
Number of Nodes	50
Transmission Range	250
Movement Model	Random Way Point Model
Maximum Node Speed	10 m/sec
Traffic Type	CBR (UDP)
No. of Wormholes	1
Malicious Nodes	2
CBR (Kbps)	64/128/192/256/320 /384/448/512/576
Packet Size	512 bytes

Fig 4: Detection Algorithm Speed Performance CBR Vs Detection Time



CONCLUSION:

The proposed technique is designed for the identification of malicious nodes in wormhole attacks in the ad-hoc network. Our trust-based mechanism is based upon N2N packet delay. The trust value of each node is calculated by observing the packet transaction between adjacent nodes. The performance verification experiment is done using

DSR and NS3 simulator [14,18]. As shown in the results the, it is clear that execution time increases gradually as the number of nodes increases but the maximum execution time of the algorithm is 0.45 ms which is a very negligible time value and maximum time is taken to detect the malicious node for a size of 50 nodes in the network is 0.472 secs which is again negligible time. These results indicate the faster performance of the algorithm. The trust value obtained for each node can be used further in making routing decisions and choosing the most trustworthy route and avoiding malicious nodes.

REFERENCES:

[1] S. Corson, J. Macker., "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC2501, 1999.

[2] L. Zhou, Z. J. Haas., "Securing Ad Hoc Networks". IEEE Network, 13(6): 24-30, 1999.

[3] Yongguang Zhang, Wenke Lee. " Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11, 2000.

[4] Y. C. Hu, A. Perrig, and D. B. Johnson., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in Proc. INFOCOM, Vol. 3, pp. 1976-1987, 2003.

[5] Capkun. S., Buttyan. L. & Hubaux. J. P., "SECTOR: secure tracking of node encounters in multi-hop wireless networks", in Proc. First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32, 2003.

[6] L. Hu and D. Evan., "Using Directional Antennas to Prevent Wormhole Attacks", In Network and Distributed System Security Symposium, San Diego, California, USA,2004,pp.2.

[7] Khalil, S. Bagchi, N. B. Shroff., "A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network", Proceedings of the 2005 International Conference on Dependable Systems and Networks,2005, 0-7695-2282-3/05.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, and MichalisFaloutsos. , "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, pp. 75-84, 2006.

[9] P. Van Tran, L. X. Hung, Y. K. Lee, S. Lee, and H. Lee,. "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks", 2007 4th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2007, pp. 593–598, 2007.

[10] Saurabh Gupta, Subrat Kar, S Dharmaraja. ,"WHOP: Wormhole Attack Detection Protocol using Hound Packets", IEEE, 978-1-4577-0314-0/11,2011.

[11] Dhruvi Sharma, Vimal Kumar, Rakesh Kumar. "Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET", Computational Intelligence in Data Mining. Volume 2. Volume 411 of the series Advances in Intelligent Systems and Computing pp 475-485., Springer, 2015.

[12] Sayan Majumdar, Prof. Dr. Debika Bhattacharyya., "Mitigating Wormhole Attack in MANET using Absolute Deviation Statistical Approach", IEEE 8th Annual Computing and Communication Workshop and Conference, pp 317-320,2018.

[13] V. Kavitha, T.Sujithra, D.Lavanya.," Trust Based Reliable Routing Protocol for Manets", International Journal of Innovative Technology and Exploring Engineering (IJITEE), SCOPUS, pp. 1595-1598,2019.

[14] David B. Johnson, David A. Maltz, and Josh Broch, "The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In Ad Hoc Networking", edited by Charles E. Perkins, chapter 5, pages 139–172. Addison-Wesley,2001.

[15] Vivek Sharma Amit Baghel,Anal "ysis of AODV and DSR in Presence of Wormhole Attack in Mobile Ad-hoc Network", International Journal of Engineering Science and Technology Vol. 2(11), pp. 6657-6662, 2010,.

[16] The ns-3 network simulator. http://www.nsnam.org.