Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Formal Verification and Validates the Mobile Nodes using NNDRP

By Machha. Narender & Dr. R. P. Singh
Sri Satya Sai University of Technology and Medical Sciences

Abstract- Mobile ad-hoc networks are wireless networks and these are suitable for safety critical applications due to its ad-hoc behavior but attackers easily enter in to the network and they can access the network, so security is a crucial factor for any communication protocols, especially in mobile environment, so verifying the node that may be a malicious node or trustworthy node is a challenging task, but most of the researchers focused on the neighbor nodes distance only but they are not focused on security. This paper provides secure routing for MANET using NNDRP protocol, this protocol verify and validate the nodes with security measures.

Keywords: *MANETS, validation, AODV, NTP, NNDRP.*

GJCST-E Classification: *C.1.3, C.1.4*

Strictly as per the compliance and regulations of:

Formal Verification and Validates the Mobile Nodes using NNDRP

Machha. Narender [α] & Dr. R. P. Singh [σ]

Abstract- **Mobile ad-hoc networks are wireless networks and these are suitable for safety critical applications due to its ad-hoc behavior but attackers easily enter in to the network and they can access the network, so security is a crucial factor for any communication protocols, especially in mobile environment, so verifying the node that may be a malicious node or trustworthy node is a challenging task, but most of the researchers focused on the neighbor nodes distance only but they are not focused on security. This paper provides secure routing for MANET using NNDRP protocol, this protocol verify and validate the nodes with security measures.**

Keywords: MANETS, validation, AODV, NTP, NNDRP.

I. Introduction

Mobile Ad-hoc Networks (MANETS) are wireless mobile nodes that cooperatively form a network without underlying any infrastructure. It has become a hot topic in wireless network over the past years.The Mobile Ad-hoc Network (MANET) is a networking concept defines simple mechanism which enable mobile terminals to form a temporary fraternity without any planned coronation, or human interference.

Finding the node position is an important task in mobile networks, and it becomes particularly challenging in the presence of contestant aiming at harming the system. In these cases, we need solutions that let nodes correctly find their location in spite of attacks supplying the false location information, and verify the positions of their neighbors, so as to detect malicious nodes announcing false locations.

Mobile ad hoc network, where a prevalent infrastructure is not present, and the location data must be obtained through node-to-node communication only. Such a scenario is of particular interest, since it is open for malicious nodes to misuse or dislocate the location based services. For example, by advertising forged positions, adversaries could bias geographic routing or data gathering processes, attracting network traffic and eavesdropping or discarding. Similarly, counterfeit positions could grant adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and carriers. In this context, the challenge is to perform, in absence of trusted nodes, a fully-distributed.

Author α: Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore, Madhya Pradesh, India.
e-mail: machha.narender@gmail.com
Author σ: Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore, Madhya Pradesh, India.
e-mail: rp.singh@gmail.com

Neighbor discovery is the process in which a node present in the network computes an identity and the total number of other nodes in its proximity. Many protocols consists fundamental building block including localization, routing, and group management. Time-based communications and many media access control mechanisms rely on meticulous neighbor information. Neighbor discovery is important to the proper functioning of wireless networks.

Neighbours are usually defined as nodes that lie within radio range of each other in the wireless network. Thus, neighbour discovery may be considered as the exploration of the volume of space or neighbourhood immediately surrounding a wireless node. Nodes found within the neighbourhood are neighbours and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, sensing and localization. However, wireless communications are prone to exploitation. Attackers have the freedom to do malicious activities ranging from simple denial of service to sophisticated deception. The correctness of node locations is thus an important task in mobile networks, and it becomes particularly challenging in the presence of adversaries target at harming the system. In these cases, we require solutions that let nodes (1) correctly establish their location in spite of attacks supplying not correct location information, and (2) verify the positions of their neighbours, so as to detect antipathetic nodes announcing false locations.

In this paper, NNDRP (Neighbour Node Discovery Routing Protocol) discovers the trusted neighbour node by AODV (Ad hoc on Demand Distance Vector) and NTP (Node Transition Probability), after finding the trusted node that can be validated by passing that node information to all its neighbour nodes to update their routing tables, then only easily to find the destination route from the source node.

II. Related Work

In this [2] paper, they presented a method which exploits Time-of-Flight distance bounding and node cooperation to mitigate the problems of the previous solutions. However, the cooperation is limited to couples of neighbor nodes, which renders the protocol ineffective against colluding attackers.

In this [1] paper, the new scheme is presented for neighbor position verification (NPV) protocol which

allows nodes to validate the neighbor nodes position based on local observations, this is done only by checking whether subsequent positions announced by one neighbor and draw a movement over time that is physically possible. The limitation of this method is an adversary can fool the protocol by simply announcing false positions that follow a realistic.

In this [3] paper, an impossibility proof showing that time-based protocols will not guarantee SND unless the environment is free of obstacles and the distance between neighbors is small.

In this[4] paper, each node transmits at randomly chosen times and discovers all its neighbors in a given time with high probability, each node transmits according to predetermined transmission schedule that allows to detect all its neighbors in a given time with its probability.

In this [5] paper, the algorithm used by Omni directional antenna is 1-way and the receiver will not send any acknowledgement after receiving the discovery message. The sender delivers the DISCOVER message to advertise itself. The receivers will discover one neighbor, if it receive the DISCOVER message properly in the listen state, The Omni directional antennas have drawbacks like decreased gain, increased signal distraction, high bandwidth consumption, and increased noise. Directional antenna requires longer transmission range and high. They strongly reduce jamming susceptibility and signal interferences in unnecessary directions.

This [7] paper, AODV protocol finds the node in source-destination rout, but it cannot find the whether it is a trust node or malicious node.

III. Proposed Protocol

NNDRP (Neighbor Node Discovery Routing Protocol) finds the trust node with the help of AODV [7] (Ad hoc On Demand Distance Vector) and NTP [6] (Node Transition Probability) protocols, AODV protocol finds the neighbor node in the source to destination route, but that node can be verified by NTP protocol, whether it is a malicious node or trust node and it can be validated by sending trust information to all neighbor nodes to update in their routing table.

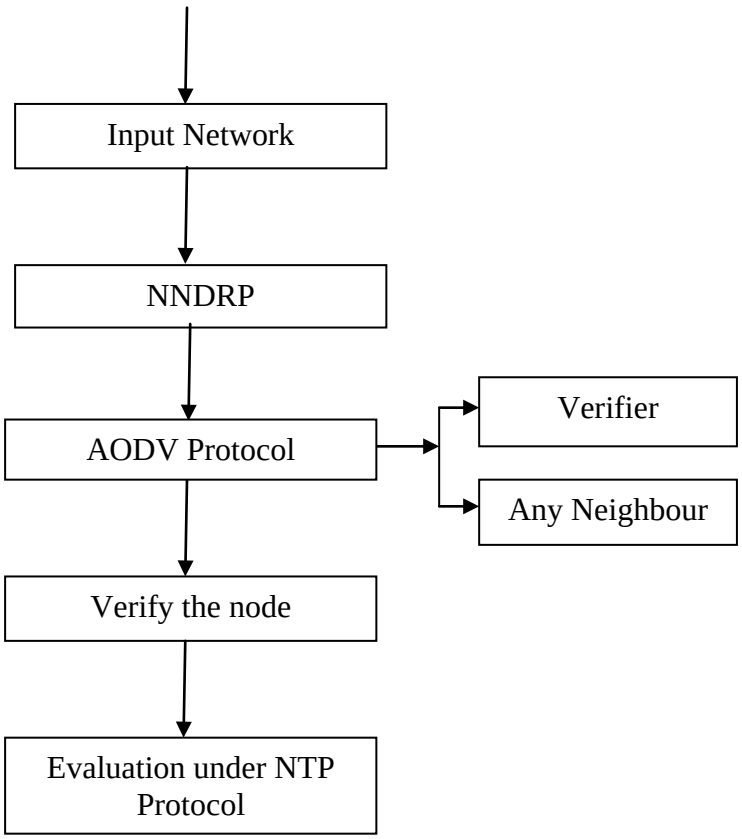

Figure 1: Proposed Architecture

AODV protocol sends a message to find a neighbour node, that message consists of rout request (RREQ),rout reply(RREP),rout error(RERR) and for checking the link status(HELLO)

In a network, after finding a node in the source-destination route by AODV protocol, to find whether it is a trust node or malicious node, that can be found by NTP protocol, it determines node based on the

probability, normally the nods lie within the verifier node's proximity for longer time, thereby improving the stability of the node, so verifier uses less control packets to determine the route between two nodes. The proposed algorithm adapts quickly changes in routing when host movement is frequent. NTP based routing algorithm, which determines the route on replied information from a particular node replied and reply that same information to all of it neighbours. In this algorithm, verifier floods a control packet, if it does not have neighbour nodes information and has data to send. The verifier table is computed based on the received replies and we choose the node, which is replied with maximum replies for more times as neighbor. By choosing that neighbour node, route table is computed for the Source to Destination. We have assumed that a node within the other node's proximity then we can say i.e. a neighbor node,

When a node in a network receives a number of route requests that is greater than the threshold value by a specific source to a destination in a particular time interval $T_{interval}$, the node is declared as malicious and the message is sent to all the nodes in a network. If any node is generating the control packets more than the threshold value in a particular time interval $T_{frequency}$, this node service can be treated as denial of service. If the source does not receive any reply from the destination for a particular time interval $T_{wait.}$, then that node can be treated as malicious node.

We can determine the crisp value for the different traffic range of the mobile nodes based up on the input parameters such as queue length (QL), data rate (DR), and item size(IS) for the Node Transition Probability protocol.

IV. Traffic Levels

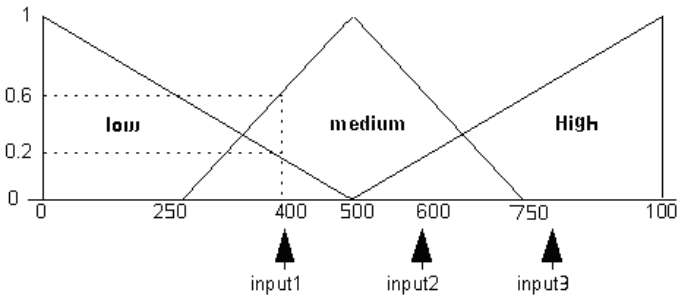

Figure 3: Three levels of input.

The above figure shows the three traffic levels based upon the input parameters after rule base is selected and sorted for various traffic levels.

a) Rule base

Rule base is designed for the fuzzy model as low-level, medium-level and high-level based on the input traffic level that is shown in table 1, 2 and 3 respectively.

Low level:

Table1: Rule Base for low level range

Rules	Queue length	Data rate	Item size	Traffic range
Rule1	Low	Low	Low	Low
Rule2	Low	Low	High	Low
Rule3	Low	Low	Medium	Low
Rule4	Low	Medium	High	Low
Rule5	Low	High	Low	Low
Rule6	Low	Medium	Low	Low
Rule7	Low	High	Medium	Low
Rule8	High	Low	Low	Low
Rule9	Medium	Low	Low	Low

Medium level:

Table 2: Rule Base for Medium level range

Rules	Queue length	Data rate	Item size	Traffic range
Rule10	Medium	Medium	Medium	Medium
Rule11	Medium	Medium	Low	Medium
Rule12	Medium	Medium	High	Medium
Rule13	Medium	Low	High	Medium
Rule14	Medium	Low	Medium	Medium
Rule15	Medium	High	Medium	Medium
Rule16	Medium	High	Low	Medium
Rule17	Low	Medium	Medium	Medium
Rule18	High	Medium	Medium	Medium

High level:

Table 3: Rule Base for High level range

Rules	Queue length	Data rate	Item size	Traffic range
Rule19	High	High	High	High
Rule20	High	High	Low	High
Rule21	High	High	Medium	High
Rule22	High	Medium	Low	High
Rule23	High	Low	High	High
Rule24	High	Medium	High	High
Rule25	High	Low	Medium	High
Rule26	Low	High	High	High
Rule27	Medium	High	High	High

In order to find the crisp value, we have framed 27 rules based on the three input parameters QL, DR and IS. Now based upon the crisp value output, the threshold parameter associated with respect to the traffic pattern in any routing protocol can be changed to achieve desired flow control. In order to improve the Intrusion detection model and the intrusion response model crisp can be used to reduce the malicious node activity in the given 'MANET'. Packet size, queue length are selected for fuzzy parameters of the data packets, data rate, power margin of nodes, and mobility range of nodes etc., a rule base is generated based upon these parameters.

V. Intrusion Detection Method

A node sends an intrusion (or anomaly) status request to a neighboring node, and then each node (including the initiation node) propagates the intrusion or anomaly status information. Then each node verifies whether the majority of the received reports indicate an intrusion or anomaly; if yes, then it concludes that the network is under attack. Any node that detects an intrusion then initiates the response procedure throughout the network.

If any node identifies that another node is compromised, when its *malcount* exceeds the crisp value of the fuzzy approach (case-2) or threshold value as for (case-1) for allegedly compromised node. In such cases, it transmits this information to the entire network through a Mal packet. If other nodes also suspect that the node which has been detected, is compromised, it reports its suspicious to the network through a ReMal packet.

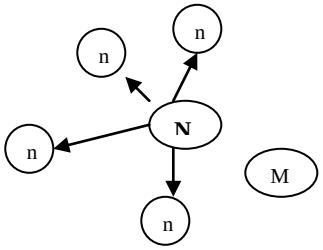

Figure 4: Mal packets generation

Audited data from other nodes cannot be trusted and should not be used because the compromised nodes can send false data. However, the compromised nodes have no chance to send reports of intrusion or anomaly because the intrusion response may result in their expulsion from the network. Therefore, unless the majority of the nodes are compromised, in this case one of the legitimate nodes will probably be able to detect the intrusion with strong evidence and will respond, the above scheme can detect intrusion even when the evidence at individual nodes is weak.

VI. Intrusion Response Method (IRM)

If two or more nodes report about a particular node, Purge packet is transmitted to isolated node in the network.

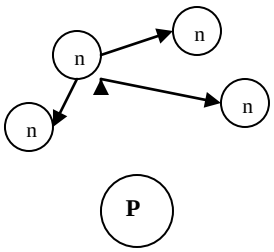

Figure 5: Purge packets transmission

All nodes look for a newer route through compromised node. All packets received from the compromised node are dropped. Any node that detects locally known intrusion or anomaly with strong evidence (i.e., the detection rule triggered has a very high accuracy rate), can determine independently that the network is under attack and can initiate the response. Purge packet is send to all the nodes in the network so that all nodes in that network becomes aware of the malicious or anomaly node and discards all the data packets and control packets from that node, through the purge packet all nodes change their rout table entry, purged node is detected from the neighbor node routing table and check the table for the neighbor nodes.

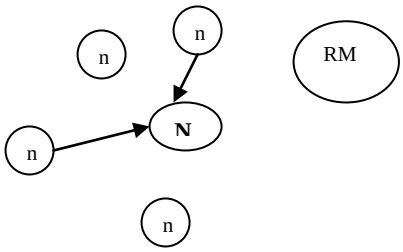

Figure 6: ReMal packets generation

VII. Implementation

The proposed security measures were implemented using NS2 as the simulator. The implementation part consists of following steps:

a) Creation of Malicious Nodes

Out of N nodes 30% of the nodes were made malicious in a network. In a network the nodes were selected randomly as malicious node, which generate more Route Requests (RR) than the normal value. Normally the nodes generate route requests for a proper rout is not known to the destination when data is present in their buffer. The randomly selected nodes were made to generate more number of route requests irrespective of their buffer data and for route discovery. Randomly each malicious node generates a variable number of route requests to another in the network.IDM and IRM operations are done cooperatively by a group of nodes when the confidence percentage level is very low. When the confidence level is very high the alleged node is directly purged from the network increasing the efficiency of the method and thereby decreasing the time taken for the detection and response modules incorporated. Thus the malicious nodes are identified through the proposed security model.

b) Method implementation

NS2 software is used to implement the method. The simulations were based on 1KM X 1KM area with 50 wireless nodes. The nodes move from a random starting point to a destination with a speed ranging from 0-20 m/sec, whenever destination is reached another destination be targeted after a pause time. The Intrusion detection and intrusion response methods are incorporated. Traffic sources are used Constant Bit Rate (CBR) with each data packet 512 bytes size, 15 nodes in the network were made malicious, sources and destinations were spread randomly across the network. The mobility model used random way in rectangular field. Duration of the simulation is 900 seconds. Separate simulation was performed for the malicious node creation in the network and after the implementation of the Intrusion Detection and Response methods.

c) Performance scaling

i. *Control overhead*

The number of control packets transmitted for every data packet is noted, for routing each hop is treated as a packet. The following graph shows that the malicious nodes increase the routing load over the network as they generate the false route requests and thereby increasing the number of control packets for each data packet. After implementing the proposed security model, it considerably decreases the routing overhead by identifying the malicious nodes and eliminating them from the network and bringing the network near to normal through NTP protocol. The performance metrics of control Overhead Vs Pause Time is shown in the below figure.

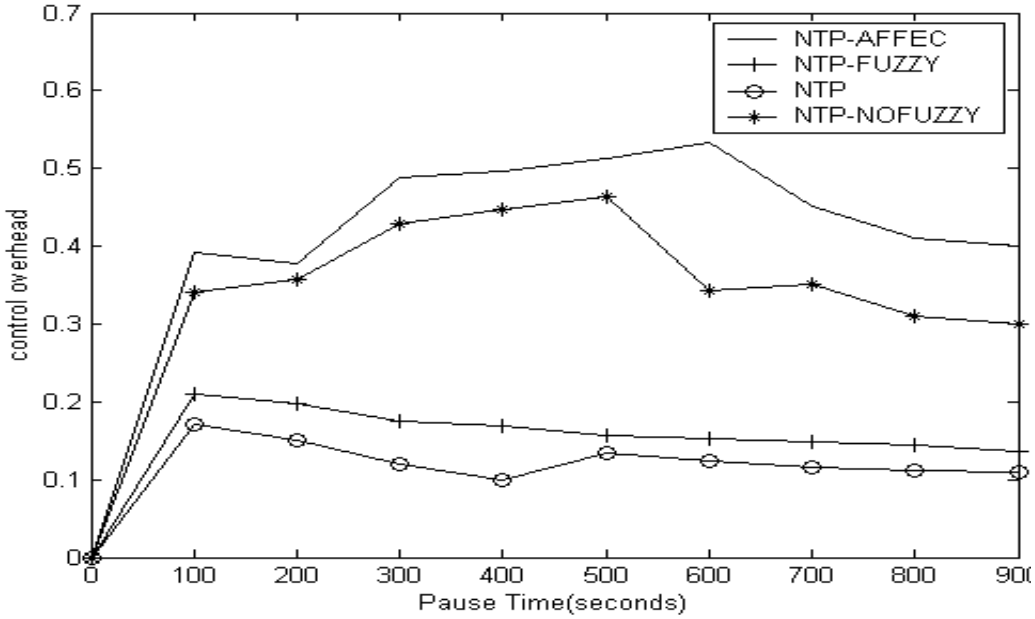

Figure 7: Control Overhead Vs Pause Time

ii. *Throughput*

The ratio of CBR packets delivered to the generated is termed as throughput. For different pairs of the source and destination pair corresponding throughput is noted. The throughputs for the NTP affected with malicious nodes are less when compared with ordinary NTP protocol. After incorporating the fuzzy approach the throughput is getting increased. The performance scaling of the throughput Vs Source-Destination Pair is shown in the figure 3.2.

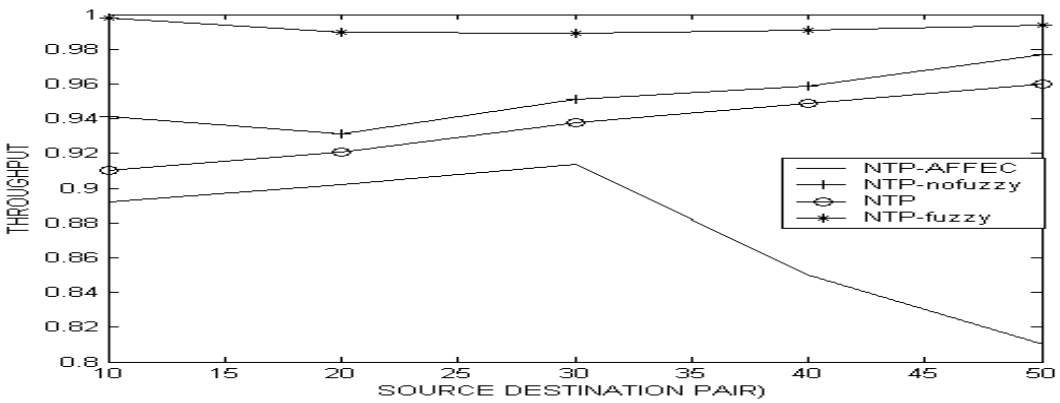

Figure 8: Throughput Vs Source-Destination Pair

iii. *Mobility*

The graph is plotted *for* different mobility ranges. The system performance has been observed in the presence of malicious nodes. The performance of the system is enhanced due to the implemented model. In the simulation misbehaving node generates false route requests, so that node corresponding packet delivery decreases. The performance metrics of Packet delivery Vs Mobility is shown in the below figure.

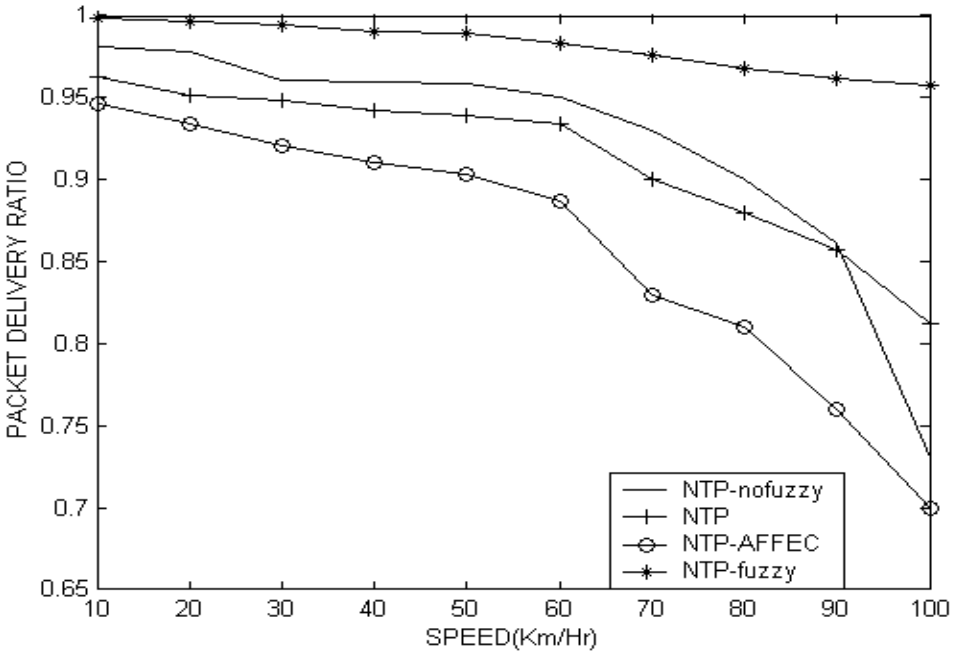

Figure 9: Packet Delivery Vs Mobility

iv. *Delay Vs Pause Time*

This is an average of delays incurred by all of the packets that are successfully transmitted. The below graph shows the malicious nodes in the network has meticulously increased end-to-end delay of the network compared to the normal network as the nodes forward the false RRs to other nodes and thereby increasing the overall time to process the control packets. The performance metrics of delay Vs Pause Time is shown in the below figure.

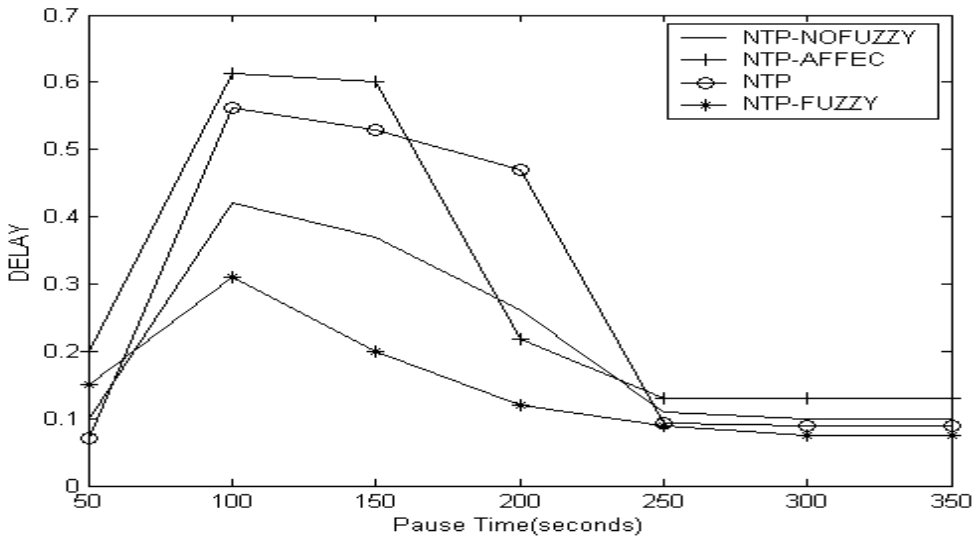

Figure 10: Delay Vs Pause Time

After incorporating the fuzzy security scheme the end-to-end delay is brought down to near normal network as intruder nodes were identified and their activities are restricted and intruder nodes are eliminated from the network.

VIII. Conclusion

The distributed false route request problem increases end-to-end delay, routing overhead, decreases the throughput and overall efficiency of the network. Our solution to this problem as successfully eliminated the intruder nodes and has brought the network performance near to the normalcy. The performance characteristics of network depicted in the graphs prove this statement.

References Références Referencias

1. T. Leinmuller, C. Maihofer, E. Schoch, F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," *ACM VANET*, Los Angeles, CA, Sept. 2006

2. S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.
3. M. Poturalski, P. Papadimitratos, and J. Hubaux, "Secure neighbor discovery in wireless networks: formal investigation of possibility," in ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2008.
4. Sudarshan Vasudevan, Micah Adler, Dennis Goessel, Fellow, IEEE, and Don Towsley, Fellow, IEEE, ACM," Efficient Algorithms for Neighbor Discovery in Wireless Networks".
5. Zhen sheng Zhang and Bo Li, "Neighbor Discovery in Mobile Ad Hoc Self-Configuring Networks with Directional Antennas: Algorithms and Comparisons".
6. Sankararajan Radha and sethu shanmugavel "Implementation of Node Transition Probability Based Algorithm for MANET and performance analysis using different mobility models" IEEE Proc, VOL5, NO.3.sept2003
7. Sonali Bhargava, Dharma P. Agarwal "Security enhancement in AODV protocol for wireless Ad Hoc networks", IEEE 2001
8. Ross, Timothy. "Fuzzy Logic with Engineering Applications", Mc Graw-Hill, New York, NY, 1995.
9. Yongguang Zhang and Wenke Lee. " Intrusion detection in wireless ad hoc networks." In the 6th international conference in mobile computing and networking (MOBICOMM'00), pages 275-283, June 2000.
10. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehaviour in mobile ad hoc networks." In 6th International Conference on mobile computing and networking (MOBICOM'00), pages 255-265, August 2000.