Security Provision For Mobile Ad-Hoc Networks Using Ntp & Fuzzy Logic Techniques

GJCST Classification
C.2.1.I.2.3

[1]Suresh Kumar [2]Machha.Narender, [3]G.N.Ramesh

[1]Assistant Professor MLEngg College. Sureshkumar1239@gmail.com
[2]Assistant Professor HITS College of Engg,machha.narender@gmail.com.
[3]Assistant Professor Bhoj Reddy Engg College, noya.ramesh@gmail.com.

***Abstract*-Ad-hoc Networks are a new generation of networks offeringunrestricted mobility without any underlying infrastructure.Primary applications of Ad-hoc networks are in military, tacticaland other security sensitive operations, where the environment ishostile. Hence, security is a critical issue. Due to the nature of Adhocnetworks, conventional security measures cannot be used.New techniques of security measures are essential for highsurvivability networks. The performance of the network will beseverely affected, in the presence of compromised nodes, whichcause undetermined and unpredictable complex failures. Thisproject is mainly to identify the misbehaviors caused by somemalicious node for NTP (Node Transition Probability) protocol,and eliminate them from the network. The performance analysis isdone based upon two cases .In first case the complete networktopology is studied and based upon it a threshold value is fixed todetect the malicious activity and eliminate it. In the second case afuzzy model is introduced so that automation of threshold can bedone for anomaly detection of malicious nodes in network withvarying topology. In contrast to the case one -- intrusion detectionmodels for ad hoc networks we have implemented an efficient andbandwidth-conscious framework that takes into distributed natureof ad hoc wireless network management and decision policies.**

Keywords- NTP, MAL, REMAL, PURGE packets, IDM, IRM, Crisp value, Security.

I. INTRODUCTION

Ad-hoc networks demand a protocol completely different from those used for wired and infrastructured wireless networks. Ad-hoc networks have their own requirements and constraints and require a protocol that takes into account these issuesand provide reliable communication under such constraints. This section explains the protocol aspects for ad-hoc mobile networks. In particular, it reveals what are the problems associated with routing in such networks. Although several routing schemes have been proposed, most of them are modified extensions of existing link-state or distance-vector based routing protocols. However, in an ad-hoc mobile network where mobile hosts are acting as routers and have both power and bandwidth constraints, conventionalprotocols that employ periodic broadcast are unlikelyto be suitable. A novel routing scheme is required toprovide efficient and high throughput communicationamong mobile adhoc networks (MANET).

The newrouting protocol-NTP that was proposed determinesroutes based on the probability that the nodes lie within the host node's proximity for a longer timethereby improving the stability of the route. Theobjective is to enhance the security issues of the NTPprotocol.

II. NTP

The proposed a new routing scheme called NodeTransition Probability (NTP) based routing, whichuses less control packets to determine the routesbetween two nodes. The proposed algorithm adaptsquickly to routing changes when host movement isfrequent. NTP based routing algorithm, whichdetermines route using the received power at aparticular node from all other nodes. In thisalgorithm, a node floods a control packet only if thereis no neighbor table and has data to send. Theneighbor table is computed based on the receivedreplies and we choose the node, which is replied withmaximum power for more times as neighbor. Bychoosing the neighbor table route table is computedfor the Source-Destination pair. The performance ofthis algorithm is studied for various scenarios andcompared their performance such as throughput,control over head and end to end delay with anexisting routing protocol. The performance resultshows that this algorithm maximizes the bandwidthduring heavy traffic with less overhead.

A. The Fuzzy Approach

In this paper the traffic pattern of the Node transition based probability protocol is to be established in terms of fuzzy logic parameters. For fuzzification process _mamdani' method is used and for defuzzification process _Mirror rule' is applied. We define the traffic levels to be low level, medium level and high level based upon the crisp value of the fuzzy security model. Intrusion detection is an important but complex task for an adhoc network. Many Artificial intelligent techniques have been widely used in intrusion detection systems. There are two main reasons for introducing fuzzy logic for intrusion detection. First, many quantitative features are involved in intrusion detection. Fuzzy set theory provides a reasonable and efficient way to categorize these quantitative features in order to establish highlevel patterns. Second, security itself is fuzzy. For quantitative features, there is no sharp delineation between normal operations and anomalies. Fuzzy episode rules allow one to create the high-level sequential patterns representing

[1]Suresh Kumar MLEngg College. Sureshkumar1239@gmail.com
[2]*Machha.Narender HITS College of Engg,machha.narender@gmail.com*
[3]G.N.Ramesh Bhoj Reddy Engg College, noya.ramesh@gmail.com.

normal behavior. With fuzzy spaces, fuzzy logic allows an object to belong to different classes at the same time. This concept is helpful when the difference between classes is not well defined. This is the case in theintrusion detection task, where the differences between the normal and abnormal classes are notwell defined. Thus the intrusion detection problem(IDP) is a two-class classification problem: the goalis to classify patterns of the system behavior in twocategories (normal and abnormal), using patterns ofknown attacks, which belongs to the abnormal class,and patterns of normal behavior. In fuzzy logic, fuzzysets define the linguistic notions, and membershipfunctions define the truth-value of such linguisticexpressions.

B. Fuzzy Algorithm

We can determine the crisp value for the differenttraffic range of the mobile nodes based upon thequality of service parameters for the given Node
Transition Probability protocol [6]
Input (1) --------- Queue length (QL)
Input (2) --------- Data rate (DR)
Input (3) --------- Item size (IT)
Range of the Input levels
Now based upon the input levelsselected the _Rule base' is sorted output for varioustraffic levels. Membership graph for the three levelsof input is shown in the figure 2.5.1.

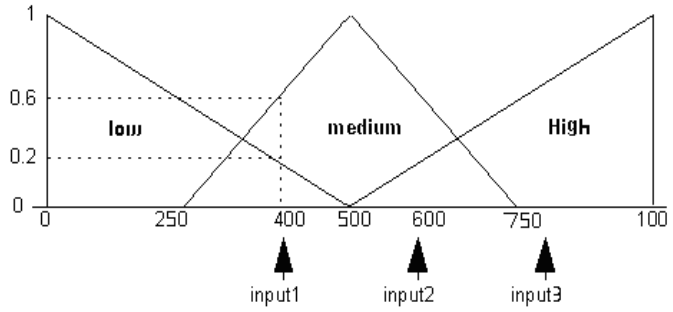

Figure: 2.2.1: Membership graph for the three levels of input.

Rule base:
With respect to the different levels of input traffic therule base for the fuzzy model is framed as low-level,medium-level and high-level and is shown in table2.5.1, 2.5.2 and 2.5.3 respectively.

Low level:

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

Table: 2.2.1 Rule Base for low level range

Medium Level

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

Table: 2.2.2 Rule Base for Medium level range

High level

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

Table: 2.2.3 Rule Base for High level range

Thus for the three input parameters quelength, datarate and the packet size we have framed 27 rules fordetermining the crisp value. Now based upon thecrisp value output the threshold parameter associatedwith respect to the traffic pattern in any routingprotocol can be changed to achieve desired flow
control. The Intrusion detection model and theintrusion response model can be improved using this_crisp value' to reduce the malicious node activity inthe given _MANET'.The fuzzy logic parameters canbe selected as the packet size, queue length of thedata packets, data rate, power margin of nodes, andmobility range of nodes etc., In this paper queuelength, data rate, packet size are taken as the fuzzyparameters, a rule base is formed based upon these
parameters. The rule base has three level of rangesbased upon the fuzzy parameters selected todetermine the crisp value of the traffic range for thegiven Node Transition Probability model. Now, thisfuzzy approach for security enhancement of NTPprotocol is the main source for the IDM& IRMmodel.

C. Algorithm For Intrusion Detection Model

The node sends to neighboring node an intrusion (oranomaly) state request. Each node (including theinitiation node) then propagates the state information,indicating the likelihood of an intrusion or anomaly,to its immediate neighbors. Each node thendetermines whether the majority of the receivedreports indicate an intrusion or anomaly; if yes, thenit concludes that the network is under attack.

Anynode that detects an intrusion to the network can theninitiate the response procedure.
A node identifies that another node is compromised,when its malcount exceeds the crisp value of thefuzzy approach or threshold value as for (case-1) forallegedly compromised node. In such cases, itpropagates this information to the entire network bytransmitting a Mal packet. If other nodes also suspectthat the node, which has been detected, iscompromised, it reports its suspicion to the networkby transmitting a ReMal packet.

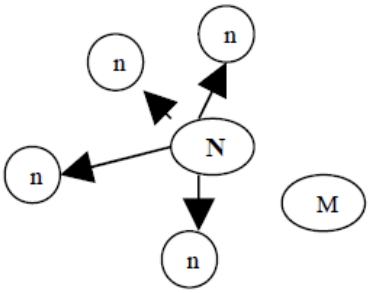

Figure: 2.6.1 Generation of mal Packets

The rationales behind this scheme are as follows.Audit data from other nodes cannot be trusted andshould not be used because the compromised nodescan send falsified data. However, the compromisednodes have no incentives to send reports of intrusion,anomaly because the intrusion response may result intheir expulsion from the network. Therefore, unlessthe majority of the nodes are compromised, in whichcase one of the legitimate nodes will probably be ableto detect the intrusion with strong evidence and willrespond, the above scheme can detect intrusion evenwhen the evidence at individual nodes is weak.

D. Algorithm For Intrusion Response Model

The following steps are taken after a purge packet issend to all nodes regarding the malicious node:

i. All the nodes in the network are made awareof the malicious node.
ii. All the data, control packets from the purgednode is dropped.
iii. A signal for route table entry modification issend to all the nodes.
iv. The purged node is deleted from theneighbor table and seen table for theneighbor nodes.

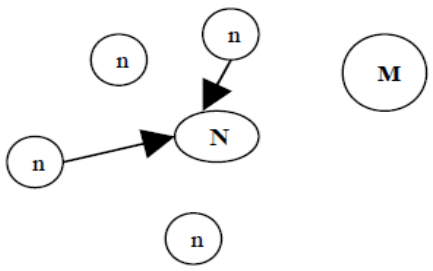

Figure: 2.8.1. Generation of Re-Mal packet by the nodes

E. Implementation

The proposed security measures were implementedusing GloMoSim as the simulator. Theimplementation part consists of following steps:

i. Creation of Malicious Nodes

Out of N nodes in the network 20% of the nodes weremade malicious. In the network the malicious nodesare the nodes, which generate more of RouteRequests than the normal value [3]. These nodeswere selected randomly. Normally the nodes generateroute requests when data is present in their buffer anda proper route to the destination is not known. Therandomly selected nodes were made to generate morenumber of route requests irrespective of their bufferand route discovery status. Each malicious node inthe network generates a variable number of routerequests to another randomly. The above said IDSIRSoperations are done cooperatively by a group ofnodes when the confidence percentage level is verylow. When the confidence level is very high thealleged node is directly purged from the networkincreasing the efficiency of the model and thereby decreasing the time taken for the detection andresponse modules incorporated. Thus the mal nodesare identified through the proposed security model.

III. PERFORMANCE METRICS

A. Control Overhead

The number of control packets transmitted for everydata packet is noted down. Each hop of the routingpacket is treated as a packet. The following graphshows that the malicious nodes increase the routingload of the network as they generate the false routerequests and there by increasing the number ofcontrol packets for each data packet transmitted.After implementing the proposed security model, itconsiderably decreases the routing load byidentifying the malicious nodes and eliminating themfrom the network and bringing the network near tonormal NTP protocol. The performance metrics ofcontrol overhead Vs Pause Time is shown in thefigure 3.1.

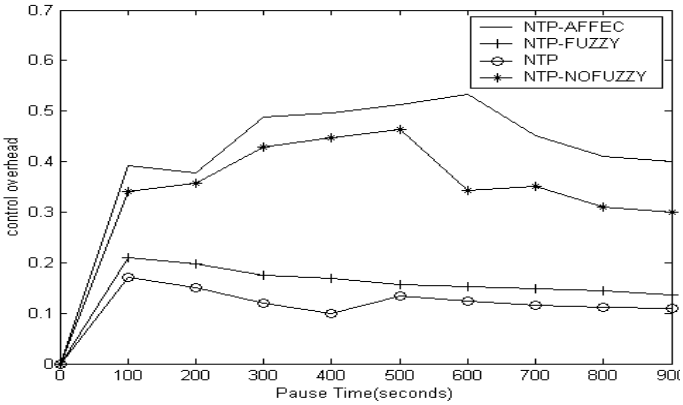

Figure 3.1: Control Overhead Vs Pause Time

B. Packet Delivery Fraction

This is the ratio of CBR packets delivered to thatgenerated and is measured as throughput. Fordifferent pairs of the source destination paircorresponding throughput is noted down. Thethroughputs for the NTP affected with malicious nodes are less when compared with ordinary NTPprotocol. After incorporating the fuzzy approach thethroughput is getting increased. Thus we prove thatfuzzy approach is better than direct assignment ofthreshold for anomaly detection. The performancemetrics of throughput Vs Source-Destination Pair isshown in the figure 3.2.

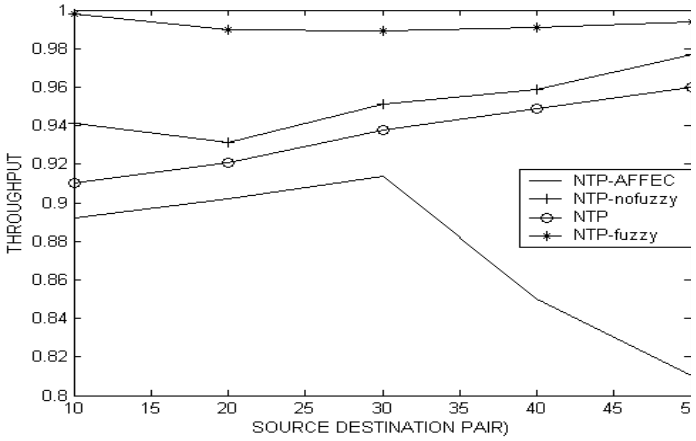

Figure 3.2: Throughput Vs Source-Destination Pair

C. Mobility

For different ranges of mobility the graph is plotted.The system performance has been observed in thepresence of malicious nodes and measured. Theperformance enhancement is due to the implementedmodel. In the simulation misbehaving node generatesfalse route requests. So the corresponding packetdelivery decreases for it. The performance metrics ofPacket delivery Vs Mobility is shown in the figure3.3.

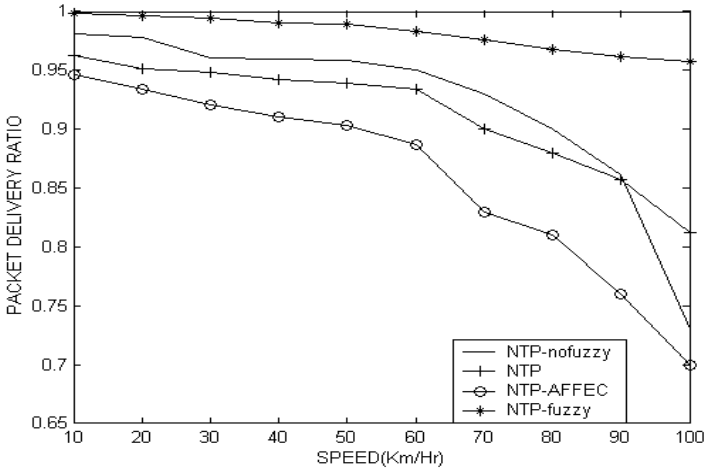

Figure 3.3: Packet Delivery ratio Vs Mobility

D. Average End To End Delay

This is the average of delays incurred by all packetsthat are successfully transmitted. The following graphshows that the malicious nodes in the network hasphenomenally increased the end-to-end delay of thenetwork compared to the normal network as thenodes forward the false RREQs to other nodes andthereby increasing the overall time to process the control packets. The performance metrics of delay VsPause Time is shown in the figure 3.4.

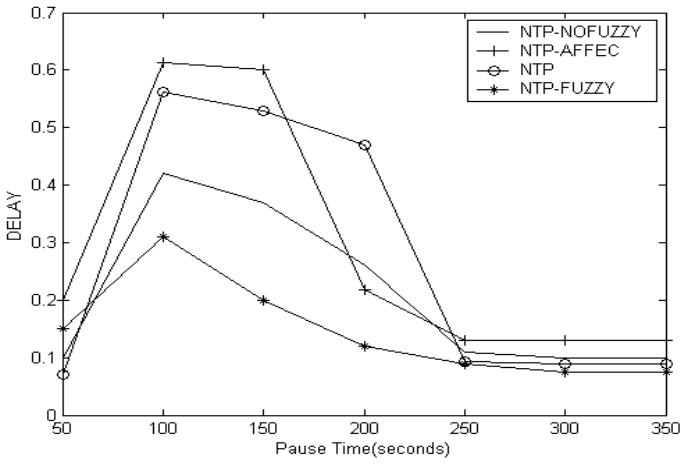

Figure 3.4: Delay Vs Pause Time

After incorporating the fuzzy security scheme theend-to-end delay is brought down to near normalnetwork as intruder nodes are identified and thereactivities are restricted and intruder nodes areeliminated from the network.

IV. Conclusion

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

V. Future Work

The future work of the paper is to extend the fuzzy automation for the security enhancement of the NTP protocol in terms of power margin and Noise margin.

VI. References

1) Charles E Perkins, Introduction to Adhoc networking, Addision Wesley, Dec 2001.
2) SankararajanRadha and sethu shanmugavel —Implementation of Node Transition Probability Based Algorithm for MANET and performance analysis using different mobility models"IEEEProc, VOL5, NO.3.sept2003

3) Sonali Bhargava, Dharma P.Agarwal Security enhancement in AODV protocol for wireless Ad Hoc networks, IEEE 2001.
4) Ross, Timothy. Fuzzy Logic with Engineering Applications. McGraw-Hill, New York, NY, 1995.
5) Ibrahim, Ahmad. Fuzzy Logic for Embedded Systems Applications. Elsevier Science, Burlington, MA, 2004.
6) Miller, Byron. The Design and Development of Fuzzy Logic Controllers. Impatiens Publications, Minneapolis, 1997.
7) 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.
8) Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In 6th International Conference onmobile computing and networking (MOBICOM'00),pages 255-265, August 2000.
9) GloMoSim User Manual, http://pcl.cs.ucla.edu/projects/domains.