Asian Journal of Information Technology 7 (5): 175-182, 2008
ISSN: 1682-3915


# Fuzzy Logic Controller Based Intrusion Handling System for Mobile Ad-hoc Networks

[1]S. Sujatha, [1]P. Vivekanandan, [2]P. Yogesh and [2]A. Kannan
[1]Department of Mathematics, [2]Department of Computer Science,
College of Engineering, Anna University, India

**Abstract:** Mobile Ad hoc network (MANET) is gaining more importance and popularity due to the proliferation of miniature yet powerful mobile computing devices. MANET is more vulnerable due to its networks characteristics, such as dynamic topology, distributed cooperation and open medium. Ad hoc On demand Distance Vector (AODV) protocol is the most popular reactive routing protocol designed for the MANET. AODV is vulnerable to both external and internal security attacks. In this study, we analyze the vulnerabilities of AODV protocol, specifically the internal attacks and we propose solutions to monitor the attack by using an Intrusion Detection System (IDS). Our solution is based on a Fuzzy Based Response Model (FBRM).

**Key words:** Ad hoc On demand Distance Vector (AODV), Mobile Ad hoc Network (MANET), Intrusion Detection System (IDS), internal attack, Fuzzy Based Response Model (FBRM)

## INTRODUCTION

The Mobile ad hoc network is a new innovation in the field of mobile communication. A MANET is considered as a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure. The mobile hosts are not bound to any centralized control like base station or mobile switching centers. As per the IETF definition (Mishra *et al*., 2004), a mobile ad hoc network is an autonomous system of mobile routers connected by wireless links.

The nature of MANETs presents substantial challenges in securing these networks. As ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration and high dependency on inherent node cooperation, intrusion detection in such systems is more complex than the system with an infrastructure. To enable constantly changing topology, these networks do not have a well defined boundary and thus, network based access control mechanisms such as firewalls are not directly applicable (Tseng *et al*., n.d). In addition, absence of centralized administration, makes bootstrapping of crypto systems very difficult. In this infrastructure-less networks, the nodes themselves perform basic network functions, such as routing and packet forwarding. It is extremely easy for malicious nodes, selfish nodes, covert channels and eavesdroppers to bring down the whole network. As a result, MANETs are vulnerable to various attacks; these attacks can be categorized using different criteria. For example, the author distinguishes between passive attacks (eavesdropping) and active attacks (alteration, fabrication, impersonation, Distributed Denial of Service (DDoS) attack) (Lou *et al*., 2004).

Another way of classification considers the identity of the attacker, whether he's an outsider or an insider (Buttyan and Hubaux, 2002). The latter is a serious problem that occurs when one of the hosts get compromised or hijacked. Usually, passive attacks can be prevented using encryption mechanisms, so in this study, we consider only the major active attacks that can be carried out in particular at routing protocol. One more way to classify the security attacks is with respect to the type of routing protocol: reactive and proactive.

The on-demand routing protocol for MANET are AODV and DSR (Baruch Awerbuch *et al*., 2004). In AODV the active attacks are: False Route Requested (FRR) attack, DDoS attack, impersonation and compromised node (Zhou and Haas, 1999). These attacks can come from any direction and target any node.

Security services, such as authentication services and access controls, can enhance the security of ad hoc networks. Nevertheless, these preventive mechanisms alone cannot deter all possible attacks (e.g., insider attackers) and in addition, they are costly to implement. Therefore, it is necessary to have other security mechanisms to deal with misbehaving internal nodes. The dynamic nature of ad hoc network suggests that prevention techniques should be complemented by

**Corresponding Author:** S. Sujatha, Department of Mathematics, College of Engineering, Anna University, India

detection techniques, which provide a second line of defense at less expense. In particular, intrusion detection and response capability are very important many of the real ad hoc networks will be deployed in aggressive environments in which legitimate nodes could be captured and used by adversaries. Intrusion detection involves the runtime gathering of data from system or packets "sniffed" from a network. The intrusion detection system techniques have been applied to privileged programs, applications and several network protocols.

This study describes our on-going research on intrusion detection and response model for MANETs using the AODV routing protocol, a widely adopted ad hoc routing protocol. This study analyzes the impact in MANET and proposed an IDS based solution supplanted with fuzzy based responding system of FRR attack. FRR attack makes congestion, flooding, DoS attack, exhaustion of bandwidth and exhaustion of resources at nodes. The exhaustion is mainly due to generating false route requests by malicious nodes at higher rate than threshold value. This FRR attack can be identified by checking or monitoring sequence number and analysing acknowledgement time and rate of route request. We propose a solution to secure this protocol based on the IDS and with an automatic fuzzy based responding system. Intrusion Detection System (IDS) detect the level of intrusion and Fuzzy Based Response Model (FBRM) takes appropriate measure to make the system immune.

We performed an extensive literature survey in the area of ad hoc network security models for various active and passive attacks. The Watchdog and Pathrater model assumes that there are no prior trust relationships (Marti *et al*., 2000). On-demand Security Routing Protocol (OSRP) scheme detects Byzantine fault using a fixed threshold scheme (Awerbuch *et al*., 2002). The On-Demand Secure Byzantine Routing protocol (ODSBR) model can detect a wide range of Byzantine attacks (black hole, flood rushing, worm hole and overlay network wormhole) (Awerbuch *et al*., 2004). Papadimitratos and Haas (2002) have showed how impersonation and replay attacks can be prevented for on-demand routing by using Secure Routing Protocol (SRP). Adaptive and Predictive Security model for MANET (APSMAN) is designed using a fuzzy feedback control approach. The model is based on identifying critical system parameters for nodes in a network (Alampalayam and Kumar, 2004). The design of Flooding Attack Prevention (FAP) is used to Secure the on-demand routing protocols from the Ad hoc flooding attack (Yi *et al*., 2005).

## VULNERABILITY OF EXISTING SYSTEM

Watchdog and Pathrater model, suffers when trusted node list in ad hoc networks are also taken into account. The OSRP scheme does not provide means of protection from DoS attacks. The ODSBR performance decreases when it has to detect and avoid a large number of adversarial links. In APSMAN model they design only for two attacks: routing loop attacks (active attack), Packet mistreatment attack (passive attack). FAP model also does not perform as desired under some overloaded conditions.

## PROBLEMS WITH FALSE ROUTE REQUEST (FRR)

Let us consider an active attack (false route request attack) by an intruder who sends frequent unnecessary route request to the neighbour nodes and this attack causes flooding of RREQ packets in the whole network and consumes lot of resources of network. This attack is identified when the nodes in the network receive a large number of route requests greater than a threshold count for a specific node to destination in a particular time interval. The specific node is declared malicious.

Basic on-demand mechanisms of route discovery and route maintenance are available in AODV protocol (Perkins and Royer, 1999). That is, a route is discovered only when it is needed. Figure 1 describes a network with nodes A to I, let node A be the source node and if node A wants to send data packets to destination node I to which it has no available route, it broadcasts a RREQ packet to its neighbour nodes B, C and D. Correspondingly nodes B, C and D send route requests to their neighbour nodes. If node C sends so many unnecessary RREQ in a small time frame, the other legitimate nodes B and D may not be able to get route reply from the neighbor node because of network congestion caused by node C. This type of attack is reflected in some of the parameters such as:

**Route request rate:** Due to malicious node in routing protocol or table, the source node is not allowed to create a route or send packets to the legitimate users. Malicious node sends large number of route requests in a particular time which exceeds the threshold value which in turn leads to network congestion and hence the genuine nodes suffer. It also restricts creation of new route in the network which would indicate the possibility of a FRR attack.

**Sequence number:** Malicious node in routing protocol or table creates a false sequence number which already

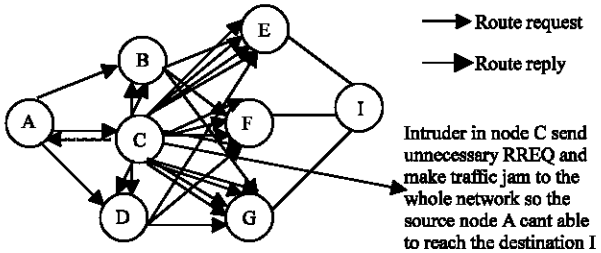


Fig. 1: Route request attack

exists in the routing table. This breaks the communication between other genuine nodes to create new route in the network and this would also indicate the possibility of a FRR attack.

**Acknowledgement time:** Presence of malicious node in routing protocol or table causes loss of the route acknowledgement from the neighbor node in a particular time and makes the route break. This would lead to a FRR attack.

**Load pattern:** The malicious node in routing protocol or table manipulates threat level according to the load pattern like normal hours, peak hours, off peak hours causing unwanted network congestion in network.

These parameters can be used to detect and predict an active attack in network and a method or system needs to be formulated to secure the AODV protocol in ad hoc network.

## PROPOSED SCHEME FOR FRR ATTACK

The proposed scheme uses a fuzzy logic controller to secure the mobile ad hoc network by monitoring various parameters of the network listed before. If these parameters change abnormally in a given time frame, the appropriate active attack is identified using a predefined weight model and a corresponding corrective measure is initiated. In the proposed security model, an IDS agent runs at each mobile node and performs local data collection and local detection, whereas cooperative detection and global intrusion response can be triggered when a node reports an anomaly.

IDS agent finds some misbehaviour in the system which is also detected by the automated system. The automated system also detects slight undetectable misbehaviour overlooked by IDS agent and initiates corresponding response. In this research, we get the data such as the load pattern, RREQ rate, Sequence Number and Acknowledgement time from the LIDS (Local Intrusion Detection System) audit log file. By using these

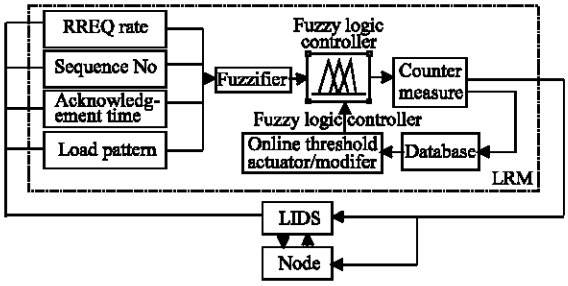


Fig. 2: Architecture of proposed model for providing security in AODV

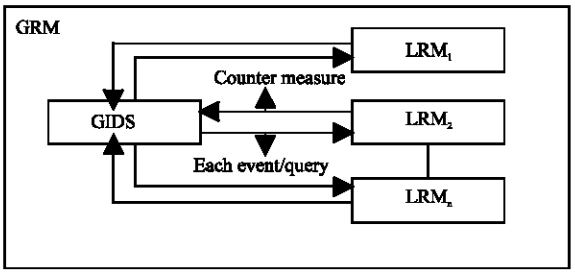


Fig. 3: Global Response module

parameters we could find the FFR attack. FBRM is used to find the intrusion level and give the counter measures to that particular malicious node and report to Global Response Module (GRM) which in turn initiates required mechanism.

Figure 2 and 3 show the architecture of the proposed security model for mobile ad hoc networks.

## IMPLEMENTATION

The proposed FBRM for securing AODV protocol network can be broadly classified into four stages such as data collection, data analysis, evaluation of LOH and initiation of counter measure.

In the following steps the basic frame work of the model is described:

**Step 1: LIDS log file:** This step collects data from the LIDS log file and also collects information from the neighbors.

**Step 2: Analysis:** This step identifies the significant parameters that relate to the attack and measures those parameters by using the fuzzy value.

The network system or node behavior can be characterised by three load patterns:

Peak hour, Normal hour, off peak hour. At any moment, a given node must be in one of the three patterns (Table 1-3). Thresholds are used to differentiate between

Table 1: Example table to illustrate the evaluation of parameters for Peak hours

| | Sequence No | | RREQ rate | | | Acknowledgement time (1/10 sec) | | Level of hacking | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No of Instance | Already existing RREQ Seq.No | New RREQ Seq.No | Low (>3/sec) | Medium (<= 5/sec) | High (5<x<10/sec) | With in TTL | After TTL | Low (<1.2) | Medium (<2) | High (>=2) |
| 1. | - | 0.5 | 0.2 | - | - | 0.5 | - | 1.2 | - | - |
| 2. | - | 0.5 | - | 0.5 | - | 0.5 | - | - | 1.5 | - |
| 3. | - | 0.5 | - | - | 1 | 0.5 | - | - | - | 2.0 |
| 4. | 1 | - | 0.2 | - | - | - | 1 | - | - | 2.2 |
| 5. | 1 | - | 0.2 | - | - | 0.5 | - | - | 1.7 | - |

Table 2: Example table to illustrate the evaluation of parameters for Off Peak hours

| | Sequence No | | RREQ rate | | | Acknowledgement time (1/5 sec) | | Level of hacking | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No of Instance | Already existing RREQ Seq.No | New RREQ Seq.No | Low (>1/sec) | Medium (<= 2/sec) | High (2<x<5/sec) | With in TTL | After TTL | Low (<1.5) | Medium (<2) | High (>=2) |
| 1. | - | 0.5 | 0.1 | - | - | 0.5 | - | 1.1 | - | - |
| 2. | - | 0.5 | - | 0.2 | - | 0.5 | - | 1.2 | - | - |
| 3. | - | 0.5 | - | - | 1 | 0.5 | - | - | 2.0 | - |
| 4. | 1 | - | 0.1 | - | - | - | 1 | - | - | 2.1 |
| 5. | 1 | - | 0.1 | - | - | 0.5 | - | - | 1.6 | - |

Table 3: Example table to illustrate the evaluation of parameters for Normal hours

| | Sequence No | | RREQ rate | | | Acknowledgement time (1/4 sec) | | Level of hacking | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No of Instance | Already existing RREQ Seq.No | New RREQ Seq.No | Low (>1/sec) | Medium (<= 2/sec) | High (2<x<4/sec) | With in TTL | After TTL | Low (<1.6) | Medium (<2.2) | High (>=2.2) |
| 1. | - | 0.5 | 0.1 | - | - | 0.5 | - | 1.1 | - | - |
| 2. | - | 0.5 | - | 0.2 | - | 0.5 | - | 1.2 | - | - |
| 3. | - | 0.5 | - | - | 1 | 0.5 | - | - | 2.0 | - |
| 4. | 1 | - | 0.1 | - | - | - | 1 | - | 2.1 | - |
| 5. | 1 | - | - | - | 1 | 0.5 | - | - | - | 2.5 |

these three patterns. And the node changes from one state to another when the load pattern changes and also the thresholds are changed depending upon the load pattern.

**Step 3: Evaluation:** This step compares the measured parameter value to the threshold value and determines the threat and sends an alarm.

In this model we used fuzzy logic approach for finding the level of hacking in the network. To calculate the level of hacking, sum of the metrics input values is collected from the IDS. This is compared with the threshold value and the vulnerability is detected depending upon the load patterns. The result of the level of hacking is calculated based on the values of fuzzy rules. For instance, the FRR attack by the malicious node would require measurement of three vulnerability factors namely number of RREQ per time interval, sequence number and acknowledgement time. The above metrics imply the nodes state. Different rules are required for different state and load patterns.

Let X is the set of represent different metric parameters that represent the attack. For finite set, X can be defined as $X = \{x_1, x_2 \ldots x_n\}$.

We have used trapezoidal membership function for fuzzy variables. The values of membership function values are real numbers in the interval [0, 1]. The membership functions for the input parameters for sequence number is classified into two: The Already existing RREQ sequence number and the new RREQ sequence number. The parameter RREQ rate is characterized into three: low, medium and high. Its ranges differ according to the load pattern. The Acknowledgement time parameter is classified into two: with in Threshold Time Limit (TTL) and after TTL.

Fuzzy system in our model uses linguistic variables to describe input and output to perform a fuzzy operation on the inputs for generating the output. Since, this model is based on a mamdani type of fuzzy controller (Lee, 1990a, b), it uses composition based inference mechanism, which combines all rules into an aggregated system output and determines the final non fuzzy control value. The Level of Hacking (LOH) is defined as:

$$LOH = \text{sequence no} + \text{RREQ rate} + \text{acknowledgement time}.$$

Table 4: Response in Peak hours

| Threshold value | LOH | Entropy level=LOH-Threshold value | System state | Response |
|---|---|---|---|---|
| 1.2 | 1.2 | 0 | Normal State | No action |
| 1.2 | 1.5 | 0.2(<=0.5) | Least Vulnerable | Action 2 |
| 1.2 | 2.0 | 0.8(<=1) | Most Vulnerable | Action 3 |

Table 5: Response in Off Peak hours

| Threshold value | LOH | Entropy level=LOH-Threshold value | System state | Response |
|---|---|---|---|---|
| 1.0 | 1.1 | 0.1(<0.2) | Normal State | No action |
| 1.0 | 1.6 | 0.6(<0.6) | Least Vulnerable | Action 1 |
| 1.0 | 2.0 | 1.0(>=1) | Most Vulnerable | Action 2 |

Table 6: Response in Normal hours

| Threshold value | LOH | Entropy level=LOH-Threshold value | System state | Response |
|---|---|---|---|---|
| 0.8 | 1.1 | 0.3(<=0.3) | Normal State | No action |
| 0.8 | 1.8 | 1.0(<=1.0) | Least Vulnerable | Action 1 |
| 0.8 | 2.2 | 1.4(>=1.1) | Most Vulnerable | Action 2 |

The resulting value of the LOH is characterized: low, medium or high. LOH values differ for various the load patterns.

**Step 4: Response:** This step finds the hacking level of the intruder and invokes appropriate security measure to move the system to the normal security level.

The responses for the system state is changed according to the load pattern and also the level of hacking.

Each and every load pattern has an individual threshold value. For peak hours the user defined threshold value is 1.2, for the off peak hours the threshold value is 1.0 and for the normal hours the value is 0.8 (Table 4-6).

Response is required only when the system is in least vulnerable and most vulnerable state.

**Action 1:** If the attack is detected and the entropy level is less than or equal to 1.0 under normal hours or the value less than 0.6 under off peak hours, it is identified as the least vulnerable state and necessary precautions are taken to prevent further damage.

The actions are:

- Verify the correct way of sending RREQ
- Automatic modification of the routing table information to the original state, in order to bring the system to original state.

**Action 2:** The action 2 is invoked when the result value is less than 0.5 in the peak hours, greater than or equal to 1 in the off peak hours and greater than or equal to 1.5 in the normal hours. The system is identified to be in least vulnerable state or most vulnerable state depending upon the values. The actions are:

- Identify the misbehavior node and isolate the malicious node (or) delete the path containing the malicious node.
- And try to modify the routing table information to the original state.

**Action 3:** This response is triggered when the value is less than or equal to 1 in the peak hours. The system is identified to be in most vulnerable state. The actions are:

- Terminate the malicious node from the network.

**Algorithms**

**Algorithm 1:** Analysis based on Sequence No
Step 1: Received a RREQ.
Step 2: Compare the sequence no of RREQ from (n-1) with routing table of nth node.
Step 3: If sequence no (n-1) =sequence no (n) then discard the RREQ and break.
Step 4: Update the sequence no in the table with a new RREQ.

**Algorithm 2:** Calculation of the RREQ Rate
Step 1: Initialize a counter for no of route request.
Step 2: If the no of RREQ is greater than one per sec then identify the node as malicious and break.
Step 3: Else check sequence no and forward the RREQ to next node as per routing table.

**Algorithm 3:** Acknowledgement time
Step 1: Get the TTL for each RREQ
Step 2: Calculate the RREQ after the receipt of acknowledgement.
Step 3: If the RREQ TTL is greater than threshold value then ignore the RREQ and break.
Step 4: Else forward the RREQ to the neighboring nodes establish a new route in routing table.

A time is preset to delete the entry in the table in case the route reply is not received before the timer expires.

**Algorithm 4:** Level of Hacking
Step 1: Received a RREQ.
Step 2: Fuzzify the sequence no, RREQ, acknowledgement time based on level.
Step 3: If the total greater than threshold value given in data table then go to step 5.
Step 4: Else declare the network to be in normal state and break.
Step 5: Give corrective measure to move the system to the normal state based on data table.

## RESULTS

In this study the simulation of the model for ad hoc networks is carried out using ns2 simulator. The input parameter values are calculated and rules are framed using the fuzzy logic controller toolbox of MATLAB version 6.1 to validate the FBRM simulation adopted. We focused on the active FRR attack in these simulation experiments.

Our simulation is based on a 1000 X 1000 m flat space, with 35 nodes. The nodes in the simulation move according to the 'random way point' model with rate of topology being classified into two slabs max speed (1.5 m) and minimum speed (0.05 m), the value of which varies with respect to the load pattern. After start of the simulation, each node waits for a pause time randomly lying between 0.25 to 2 sec and then randomly selects and moves towards a destination with a speed of 10-20 m $sec^{-1}$.

Using the fis editor utility of MATLAB the network performance parameters are evaluated. The linguistic variables for sequence no, RREQ rate, acknowledgement time and LOH in MATLAB are shown in Fig. 4-7 for the case of load pattern during peak hours. The dynamic nature of the Ad-hoc network is incorporated by incrementing each parameter value in quantized steps and once the maximum range is attained the step wise decrement operation is initiated. Since, the number of decrement, increment steps and frequency for various parameters are different we get extensive combination as encountered in real time condition. According to the parameter values, the rules are framed with corresponding responses which is to be fed back to the system for counter measure. This simulation method is shown in Table 7.

The linguistic variables of membership functions for sequence number is classified into 2 and these are same for all load patterns. If the sequence no already exists in the routing table it falls under the category of already existing RREQ sequence number and it ranges from 0.5-1, else the new RREQ sequence number ranges from 0-0.5.

The membership function for RREQ rate is classified into three: low (0-0.3), medium (0.3-0.5) and high (0.5-1).

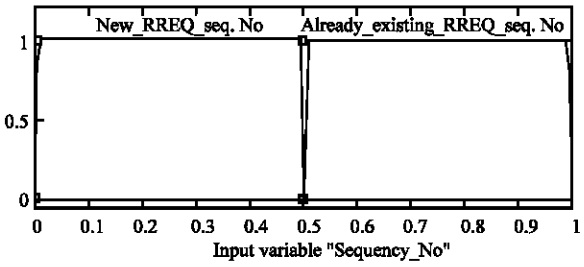


Fig. 4: Membership functions for sequence no

The membership functions for acknowledgement time is classified into 2 and these are same for all load patterns. If the neighbour node sends the acknowledgement in the threshold time limit it intimated as with-in TTL which ranges from 0-0.5. If it exceeds the threshold value, the after TTL ranges from 0.5-1.

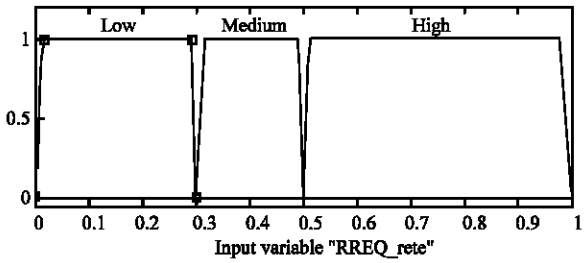


Fig. 5: Membership functions for RREQ rate

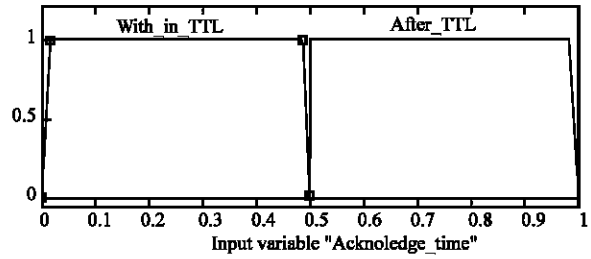


Fig. 6: Membership functions for acknowledgement time

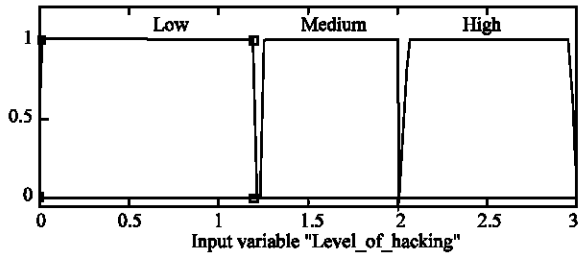


Fig. 7: Membership functions for LOH

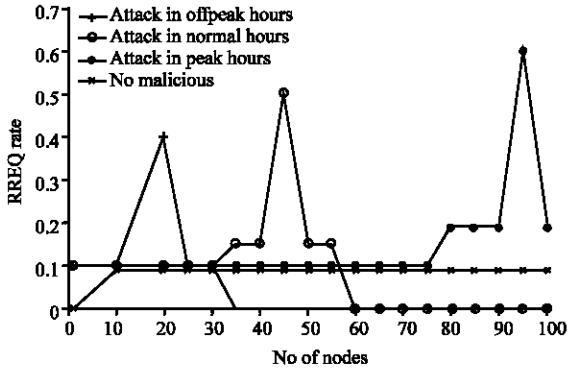


Fig. 8: Attacks in various load patterns

**Table 7: The simulation table for the ad hoc network for various load patterns**

| Peak hours | | | | Off Peak hours | | | | Normal hours | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| No of Nodes | | | | No of Nodes | | | | No of Nodes | | | |
| 20-35 | | | | 20-35 | | | | 20-35 | | | |
| Max speed range | | Min speed range | | Max speed range | | Min speed range | | Max speed range | | Min speed range | |
| 1.5-1.0 m $s^{-1}$ | | 1.0-0.5 m $s^{-1}$ | | 1-0.5 m $s^{-1}$ | | 0.5-0.25 m $s^{-1}$ | | 0.5-0.25 m $s^{-1}$ | | 0.25-0.05 m $s^{-1}$ | |
| Pause time | | | | Pause time | | | | Pause time | | | |
| 2s-1.5s | 1.5s-1s | 2s-1.5s | 1.5s-1s | 1.5s-1s | 1s-0.5s | 1.5s-1s | 1s-0.5s | 1s-0.5s | 0.5s-0.25s | 1s-0.5s | 0.5s-0.25s |
| Entropy level | | | | Entropy level | | | | Entropy level | | | |
| 0 | <=0.5 | <=1 | | <0.2 | <0.6 | >=1 | | <=0.3 | <=1.0 | >=1.1 | |
| System state | | | | System state | | | | System state | | | |
| N | LV | MV | | N | LV | MV | | N | LV | MV | |
| Response | | | | Response | | | | Response | | | |
| NA | A2 | A3 | | NA | A1 | A2 | | NA | A1 | A2 | |

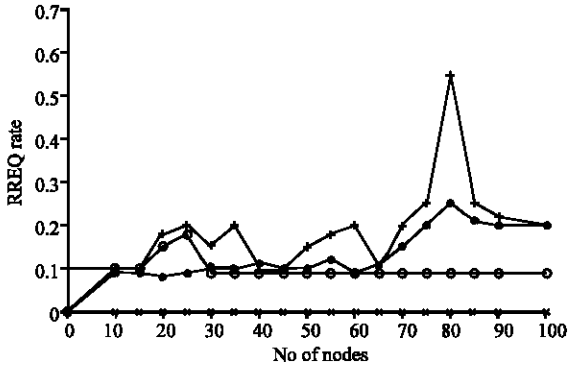


Fig. 9: Impact of RREQ in network performance

The membership function for LOH is categorized into three: low (0-1.2), medium (1.2-2) and high (2-3).

An attack in various load patterns is shown in Fig. 8. The impact of RREQs rate is the network performance over the period of time is shown in Fig. 9.

## CONCLUSION AND FUTURE WORK

In this study, we discussed active security issues of AODV protocol in mobile ad hoc networks. We have also proposed a practical and effective security FBRM model. This gathered, analysed and controlled or supervised the various threats and functional properties of an MANET using fuzzy logic controller approach. The model is based on identifying the hacking level by using the system parameters that are affected by the attacks. These parameters are constantly monitored in each and every node in the network. Experimental result of the model simulated using ns2 for the selected FRR active attack is very probable. Number of parameters to be controlled can be tailor made for specific application also this model can be extended to other protocols used in ad hoc network communication. And also we extend this work for other active and passive attacks in the ad hoc network using this FBRM model.

## REFERENCES

Alampalayam, S.K. and A. Kumar, 2004. An adaptive and predictive security model for mobile Ad Hoc Networks. Wireless Personal Commun., 29: 263-281.

Awerbuch, B., D. Holmer and C. Nita-Rotaru, 2002. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of ACM Workshop on Wireless Security (WiSe).

Awerbuch, B., R. Curtmola, D. Holmer and C. Nita-Rotaru, 2004. Mitigating Byzantine Attacks in Ad Hoc Wireless Networks. Technical Report Version 1, pp: 1-14.

Buttyan, L. and J.P. Hubaux, 2002. Report on a Working Session on Security in Wireless Ad Hoc Networks. Mobile Comput. Commun. Rev., 6 (4): 1-17.

Lee, C.C., 1990a. Fuzzy Logic in Control Systems: Fuzzy Logic Controller-Part I. IEEE. Trans. Syst. Man and Cybernetics, 20 (2): 404-418.

Lee, C.C., 1990b. Fuzzy Logic in Control Systems: Fuzzy Logic Controller-Part II. IEEE. Trans. Syst. Man and Cybernetics, 20 (2): 419-434.

Lou, W., W. Liu and Y. Fang, 2004. SPREAD: Enhancing data confidentiality in mobile Ad-Hoc networks. IEEE, 0-7803-8355-9/04, pp: 2404-2413.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proc. 6th Ann. Int. Conf. Mobile Comput. Networking, Boston, MA, pp: 255-265.

Mishra, A., K. Nadkarni, A. Patcha and V. Tech, 2004. Intrusion Detection in Wireless Ad Hoc Networks. IEEE. Wireless Commun., 1536-1284/04, 4: 48-60.

Papadimitratos and Haas, 2002. Secure Routing for Mobile Ad Hoc Networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, pp: 27-31.

Perkins, C.E. and E.M. Royer, 1999. Ad hoc On-Demand Distance Vector Routing. IEEE Workshop on Mobile Computing System and Application (WMCSA), pp: 90-100.

Tseng, C.Y., P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt, n.d. A Specification Based Intrusion Detection System for AODV. Network Associate Laboratories, Network Associates, Inc.

Yi, P., Z. Dai, S. Zhang and Y. Zhong, 2005. A New Routing Attack in Mobile Ad Hoc Networks. Int. J. Inform. Technol., 11 (2): 83-94.

Zhou, L. and Z.J. Haas, 1999. Securing Ad Hoc Networks. IEEE. Network Mag., 13 (6): 24-30.