BIJIT - BVICAM's International Journal of Information Technology
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network

Shadab Siddiqui[1], **P. M. Khan**[2] and **Muhammad Usman Khan**[3]

Submitted in June, 2014; Accepted in September, 2014

Abstract - The paper entitled "Fuzzy Logic based Intruder Detection System in Mobile Adhoc Network" is an approach to detect malicious nodes by applying fuzzy logic in Mobile ad-hoc networks. Security is a major concern in various scenarios of adhoc sensor network. Detection of malicious nodes forms an essential part of an approach to security. The proposed work uses fuzzy logic to identify the attack and malicious behavior of nodes. The proposed work will identify the attack over the network as well as provide the solution to reduce the execution time over the network. The objective of the work is to provide security in Mobile Adhoc Network. The proposed work uses AODV algorithm. This algorithm implies some fuzzy rules which is implemented on the nodes in the network. The if-then rules of fuzzy will identify the malicious node in the network. The proposed work will do comparison between the performance parameters obtained from AODV with priority based Intruder detection system with AODV implementing fuzzy logic to identify malicious nodes. The results will show great improvement of AODV with fuzzy logic over the previous algorithm. The proposed scheme is implemented using Matlab & its results show its effectiveness.

Index Terms – Fuzzy logic, AODV, Mobile Adhoc Network, fuzzy rules, attacks, RREQ- Route request, RREP- Route reply, RERR- Route error.

1.0 INTRODUCTION

As the technology is increasing day by day the popularity of wireless technology is showing a tremendous rise & therefore opening various fields of applications in the area of networking. One of the most important fields in this is MANET in which the nodes do not depend on any preexisting infrastructure. MANET consists of collection of nodes that are connected by wireless links & therefore the interconnection between nodes can change on arbitrary basis. Nodes that are within the communication range of other nodes can communicate directly without the need of wireless links whereas nodes that are far away uses intermediate nodes as relays. The book Adhoc Sensor network [1] defines the network consist of number of nodes and mobile host MH connected by wireless links. Therefore MANET can operate as a standalone implementation with an infrastructure less network. Security in Mobile Adhoc Network is very difficult to achieve due to its dynamic & infrastructure less topology & due to limitations of wireless data transmission. The existing solution applied in wired network can obtain security to a certain level but not always suitable in wireless network. Therefore wireless network has its own vulnerability that cannot be handled by wired network. Due to the different characteristics of wireless & wired network the task of providing seamless environment for it is very difficult. In Mobile Adhoc Network nodes also have limited energy storage. Mostly, they are battery equipped, with very limited recharging or with no replacement possible. Another limited resource in Mobile Adhoc Network is bandwidth. All of the above features of MANETs do pose a serious challenge which is often easier to achieve or predict in wired or infrastructure based networks. Thus, guaranteeing data safety and reliability is a serious issue..

Therefore, the decentralized nature, scalable setup and the dynamic changing topology makes adhoc networks ideal for a variety of applications ranging from military, industrial and natural to data collection machinery analysis, bio-sensing as investigated in [2], [3]. But these same features also drive the key challenges in deploying and using them such as device compatibility, connectivity issues due to varying traffic, security and survivability of nodes in the network

2.0 FUZZY LOGIC

Boole [4] introduced the beautiful notion of binary sets, which is the foundation of modern digital computer but boolean logic is unable to model the human cognition and thinking process. Because of its rigid boundaries, the two valued logic is not so efficient in mapping real world situations. In order to handle real world problems Zadeh [5] introduced the concept of 'mathematics of fuzzy or cloudy quantities' followed by his seminal paper 'Fuzzy sets' [6].

Fuzzy logic is a superset of Boolean logic. Fuzzy logic uses fuzzy rules which are one of the important applications of fuzzy theory. Fuzzy logic is described as a mathematical system that uses analog input value between 0 and 1 in contrast to to digital logic. Steps for fuzzy logic are:-

1) Fuzzification*:* The aim of fuzzification is to define input variable & input membership function for each input variable.

2) Knowledge base: It classifies input according to membership values such as low, medium, high. The knowledge base consists of rules in the form of if-then rules.

3) Defuzzification (mapping): In this two graphs are used.

- Template Graph- It contains all output membership function which are maximized when they have high fuzzy rules.
- User Action Graph- It includes audit log & user profiles.

[1, 2, 3]Department of Computer Science and Engineering, Integral University, Lucknow
EMail:[1]shadabsiddiqui222222@gmail.com,
[2]pmkhan@hotmail.com and [3]usmanintegral@gmail.com

INPUT
Processing Stage
OUTPUT

Figure1: Fuzzy Controller

Fuzzy logic deals with reasoning which is approximate instead of fixed. The value in truth table of fuzzy logic ranges between 0-1. It is a problem solving methodology from simple microcontroller to large control systems. Fuzzy logic gives a simple way to arrive at definite conclusion based upon noisy, ambiguous or missing input information.

2.1 Fuzzy logic toolbox

Fuzzy logic toolbox can create and edit fuzzy inference systems. These inference systems can be created using command line functions or by using graphical tools. By using simulink we can test our fuzzy system in simulation environment. The toolbox can run C programs without using simulink. This is possible because of fuzzy Inference engine which reads the fuzzy systems.

2.2 Fuzzy sets

Fuzzy sets are the sets without any fixed defined boundary. It contains elements with degrees of membership functions. Fuzzy sets is a pair (v, m), where v is a set & m : v→[0,1]. Fuzzy set theory assesses the membership function of elements in a set which is described by the help of membership function in the interval [0, 1].

2.3 Membership Function

It is the curve or square graph which defines the mapping of each input point to membership value between 0 and 1.

Ex: Consider a fuzzy sets is the set of tall people. We say from 3 ft to 9 ft word 'tall' will correspond to curve which defines the degree to which the person is tall. If the tall people in the set are within the boundary of classical set then we can say that all people taller than 6 ft are considered tall.

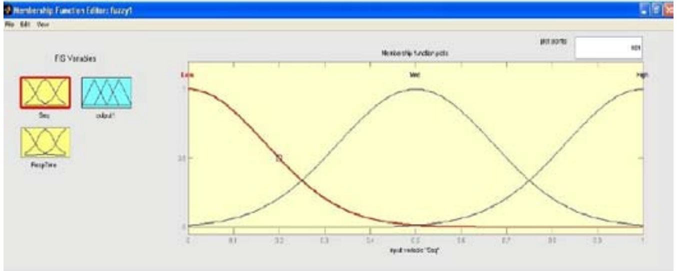


Figure 2: Fuzzy Input Membership function

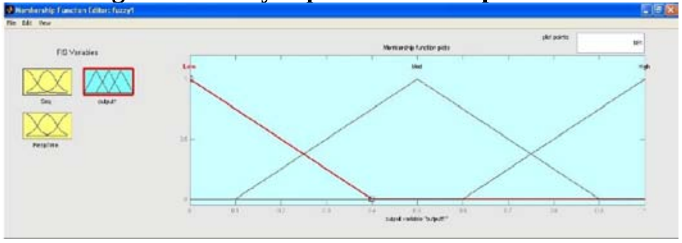

Membership Function Editor: fuzzy1
File Edit View
FIS Variables
Seq
output1
RespTime
Membership function plots
plot points
Low
Med
High
output variable "output1"

Figure 3: Fuzzy Output Membership Function

2.4 If-then rules

The if-then rules statements can formulate the conditional statements that consist of fuzzy logic. A single fuzzy rule comprises of:

If x is A then y is B, where A& B are values defined by fuzzy sets on the range x & y respectively. The if part of the rule states x is A and is called as antecedent, and then part of the rule is y is B and is called as consequent.

3.0 AODV ALGORITHM

AODV is used basically to address routing problems in Mobile Adhoc Network. & establish communication between nodes with minimum control overhead. AODV is a reactive protocol and it does not need the discovery & maintenance of routes which are not in communication instead it discovers the routes quickly to new destinations. AODV is loop free algorithm & operates in distributed manner. This freedom of loop is acquired by using sequence number. Every node has a sequence number which increases monotonically every time there is a change in topology of the network. This sequence number also ensures that recent route is selected when a route discovery process initiates. It basically has three phases:-

3.1 Route Discovery

If the node wants to communicate with destination node then it checks if the route to destination is free &valid in the routing table. If the route is available & valid then data is sent and if it does not have the valid route to destination then the source node sends RREQ packet & sets a timer to wait for RREP. Every node on receiving RREQ packet checks whether it has verified the IP address of source & broadcast ID of RREQ. After RREQ the next step is to set reverse routes in routing table. The reverse route contains the IP address of source, the sequence number & the hops required to reach source node.

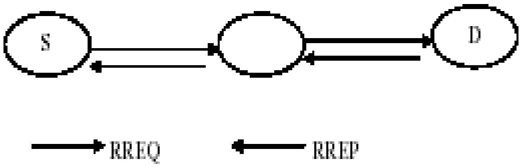


Figure 4: Route discovery in AODV

3.2 Route Maintenance

If a source node moves in between then it reinitiates the route discovery process. If a link to the node fails then that node should inform about breakage of link to source node by sending RERR message. The source again reinitiates route discovery process. In order to maintain connectivity between nodes AODV regularly send HELLO message to nodes. AODV uses sequence number to ensure freshness of the route. If there are multiple routes with same sequence number then route with smallest sequence number is chosen.

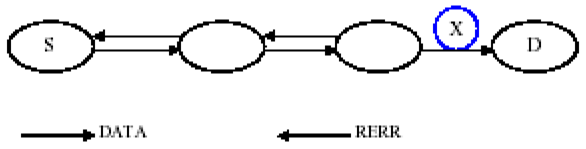


Figure 5: Route Maintenance in AODV

3.3 Data forwarding

In this process the nodes in between stores the address of neighbor from where first packet was received. If more than one copy of RREQ are received then they are discarded. When RREQ reaches the destination node it generates route reply RREP packet.

4.0 RELATED WORK

In this section we will study various national and international research papers and about the proposed techniques for malicious node detection in Mobile Adhoc Network. The research area related to this field is very large and complex. Here we will discuss some of them which are related to my proposed work.

Antonio M. Ortiz and Teresa Olivares proposed “Fuzzy Logic Applied to Decision Making in Wireless Sensor Networks” [7]. It states the application of fuzzy logic in decision making in wireless sensor network. The state that the developers should consider theoretical & practical issues when designing and implementing routing schemes. They proposed that with the use of fuzzy logic in decision making process of AODV protocol they can select best nodes to be the part of routes. Here they proposed fuzzy logic to improve the selection of routing metrics. It contains details of parameter selection, definition and fuzzy rule design. They have also showed the results in comparison to AODV by using AODV-ETX, an interesting metric used in wireless network. From results obtained they said that AODV-FL consumes less energy because it sends less messages thereby resulting in fewer collisions. Hence by using fuzzy logic as a metric in network routing improves the overall performance of the network.

B.Ben Sujitha1, R.Roja Ramani2, Parameswari3 proposed Intrusion Detection System using Fuzzy Genetic Approach [8]. It states that by using Fuzzy genetic algorithm FGA for intrusion detection we can detect new attacks and handle them. They state that IDS are effective against attacks. Various changes are done to IDS to detect new and malicious attacks. In this paper they introduced FGA. The FGA approach is based on if-then rules along with genetic algorithm. This method is tested on KDD’ 99 benchmark dataset and they are compared with already existing techniques. They state that implementation of FGA showed effective results in field of IDS. They also said that in future FGA algorithm can also be used to minimize computation time.

Sampada Chavan, Neha Dave and Sanghamitra Mukherjee proposed Adaptive Neuro-Fuzzy Intrusion Detection Systems [9]. It states that two paradign, Artificial Neural Network & Fuzzy Inference System are used for IDS. They proposed SNORT in order to perform traffic analysis & packet logging on IP network during the training phase of system. Then they constructed signature pattern database using Neuro Fuzzy learning method. They also state that 40% of original number of input variables, we can improve the performance & development time. In future IDS can also produce results by examining input from different sources.

Bharanidharan Shanmugam and Norbik Bashah Idris proposed Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks [10].They proposed a hybrid model based on fuzzy & data mining techniques which can detect any type of attack. They proposed to reduce the data retained for processing which includes selection process of attribute & to improve IDS using data mining technique. They have used KUoK fuzzy data mining algorithm which is the modified version of APRIORI for implementing fuzzy if-then rules. The proposed model is tested against DARPA 1999 data set for efficiency. The future work is to turn the system into light weight system by overcoming drawbacks such as bottleneck in packet processing & improve the performance of faster detection and alert correlation. The future work is to make this system as an open source project and get ready for real world challenges.

Devendra K. Tayal, Amita Jain and Vinita Gupta [19] proposed Fuzzy Expert System for Noise Induced Sleep Disturbance and Health Effects. They have developed a fuzzy based model in detecting noise effects on health and sleep disturbance. They have implemented their work in MATLAB 7.0.1. They have developed Fuzzy MIMO Expert system to predict the health conditions in noisy region.

This reference motivated me to apply fuzzy logic approach in my work.

5.0 PROPOSED WORK

The proposed work consists of four phases namely Path generation using AODV algorithm, applying Fuzzy logic, verification and detection of malicious nodes.

Phase One: Path generation using AODV algorithm

In this phase AODV algorithm is applied to generate path for route discovery. AODV uses all its features to generate the path from source to destination.

Phase Two: Applying Fuzzy logic

In this phase the generation of fuzzy rules takes place along with membership function. The fuzzy IF-THEN rules are applied in order to detect malicious node.

Phase Three: Verification

In this phase verification of IF-THEN rules takes place. The condition of IF statement verified by checking if the destination sequence number is much greater than source sequence number and if response time of node is greater than set threshold value then malicious node is detected

Phase Four: Detection of malicious node

In this phase we will be able to detect the malicious node by applying fuzzy rules.

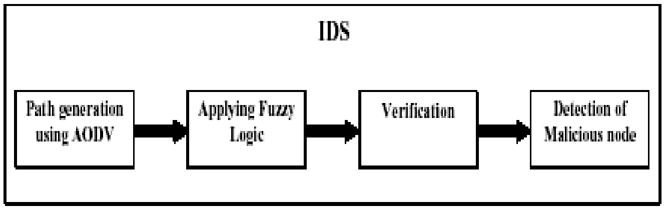


Figure 6: Proposed Fuzzy based IDS

5.1 Fuzzy Rules

Rule 1) If (source sequence is low) OR (response time is high) then output is medium

Rule 2) If (source sequence is low) AND (response time is medium) then output is high

Rule 3) If (response time is medium) then output is low.

Rule 4) If (source sequence is high) then output is low.

6.0 RESULTS AND DISCUSSION

Here we will evaluate our model Intruder Detection system in MANET using Fuzzy Logic. This system is developed to operate anywhere in any situation, therefore the experiment is carried out with same scenario with different experiments that shows the performance of system. The parameters used for simulation will be compared to the existing model.

It is very important to choose suitable parameters for system evaluation. The performance parameters will describe the result of simulation. These parameters are important as they will be used to notify what will actually happen during simulation

Our choice is using MatLab- 2010. Matlab uses the hierarichal architecture in order to define components like nodes & network. The components are defined by text based language. The components can be nested to form complex module inside each other.

Every module can be accomplished by C++ file which describe its behavior. MatLab provides many modules such as queues, tools etc. by using C++ computation. MatLab uses documentation & active discussion forums.

The experiments were carried out by MatLab-2010. The scenarios developed to carry out the tests use as parameters the mobility of the nodes and the number of active connections in the network. Node are presented previously were utilized in the experiments. The choices of the simulator are presented in table 1	Matlab-2010

Simulation Area	50*50m
No of nodes	10 to 100
Transmission range	25m
Mobility Model	Random Waypoint
Max Speed	5-20 m/sec
Traffic Type	CBR(UDP)
Data payload	512 bytes
Packet rate	2 packet/sec
No of malicious nodes	3
Simulation time	30 sec
Routing Protocol	AODV
MAC	802.11
Pause Time	10 sec
Mobility	10.70 m/s
Terrain area	100*100m

Table 1: Measurements in MATLAB

6.1 Validation in terms of metrics used for comparison

The performance comparison is based on various metrics between existing AODV with proposed AODV using fuzzy logic.

6.2 Throughput

It is defined as total no of delivered packets divided by the total duration of simulation time.

Throughput = (Packets sent / Packet Total) *100

6.3 Hop Count

It is variation in time stuck between packets inward caused by network congestion & due to route changes.

6.4 Execution Time

It is the time used by algorithm for execution

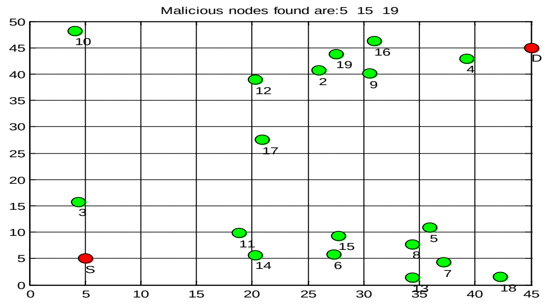


Figure 7: Displaying no of nodes in 50*50 area

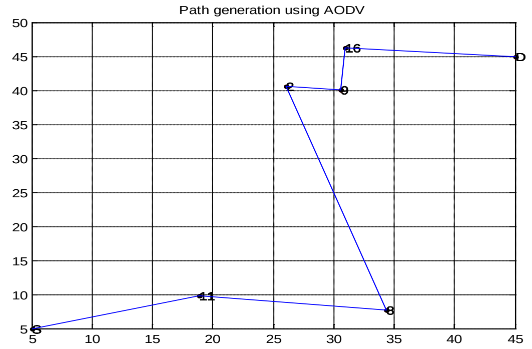


Figure 8: Line showing path from source to destination

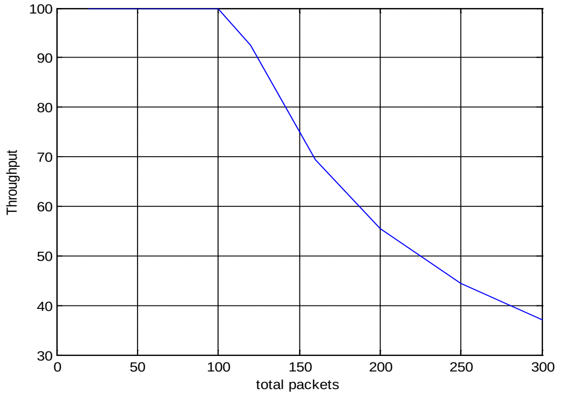


Figure 9: Graph displaying throughput

RREQ SENDS to Nodes:	Acknowledgement Received from Nodes:
11 14 6 15 17 8 5 12 2 9 19 16 4 20	11 8 2 9
Selected Path is: 1 11 8 2 9 16 20	Hop Count is: 6 Elapsed time is 1.365541 seconds. Malicious count=3

Table 2: Results showing RREQ and ACK packets along with execution time and malicious count

FIS Editor

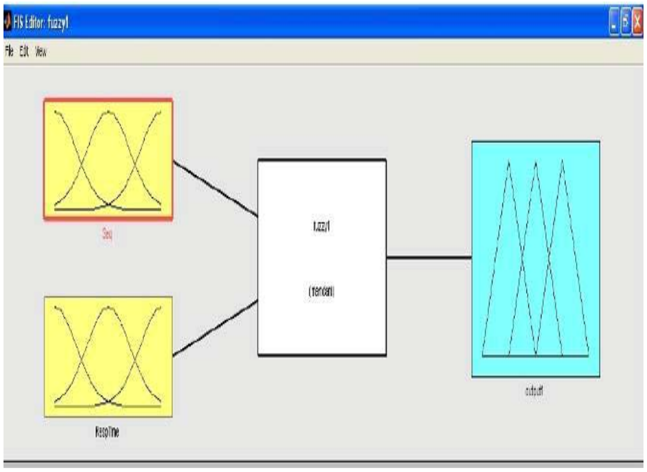
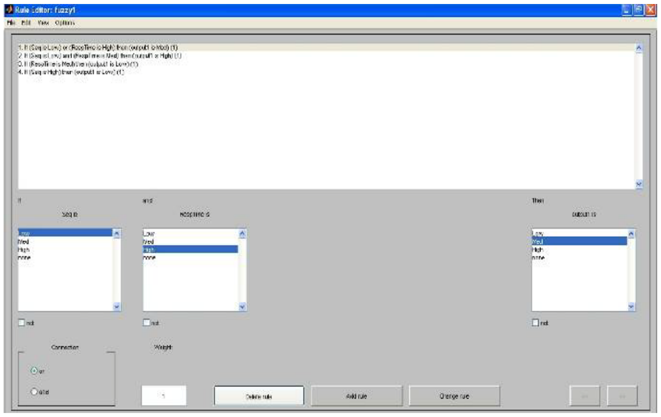


Figure 10: FIS Editor

Rule Editor



1. If (Seq is Low) or (RespTime is High) then (output1 is Med) (1)
2. If (Seq is Low) and (RespTime is Med) then (output1 is High) (1)
3. If (RespTime is Med) then (output1 is Low) (1)
4. If (Seq is High) then (output1 is Low) (1)

Figure 11: Rule Editor displaying the if-then rules used

Rule Viewer

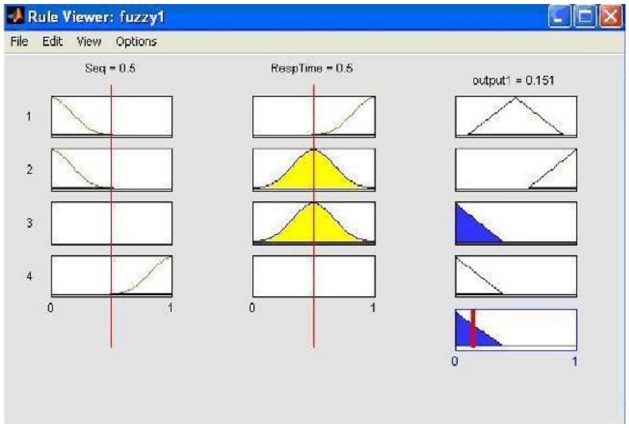
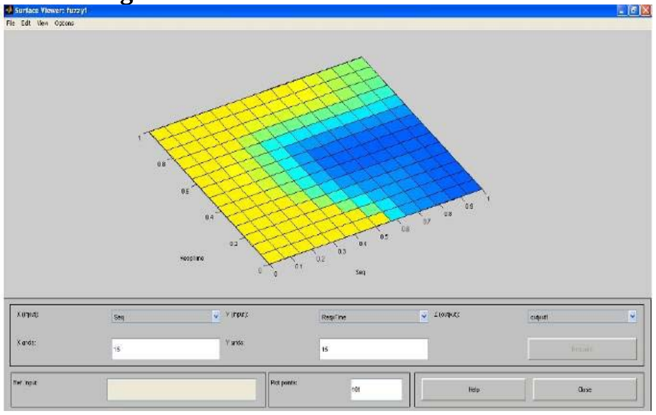


Figure 12: Rule Viewer diagram in fuzzy logic

Surface Diagram



X (input): Seq
Y (input): RespTime
Z (output): output
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101

Figure 13: Surface diagram displaying the no of malicious nodes

7.0 CONCLUSION & FUTURE WORK

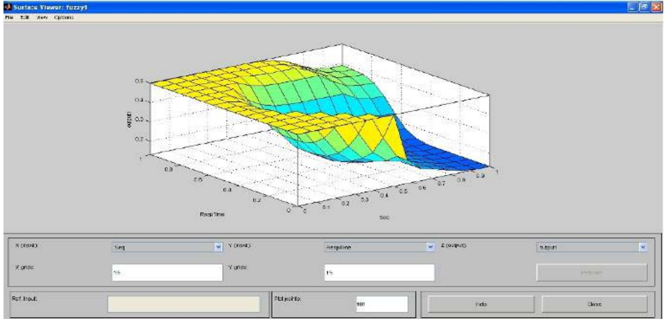
The security of MANET has gained popularity among research area. The security issues are discussed and we have analyzed the security system with our proposed model Intruder Detection System in MANET using Fuzzy Logic. This model is very efficient for protecting against attacks. Our proposed model can find the safe route and helps in preventing attack in MANET by identifying the node with sequence no & threshold value.

The proposed scheme is implemented using Matlab & its results show its effectiveness. The method will check for the difference between source sequence number & destination sequence number; if the source sequence no is greater & crosses the threshold value then that node is said to be malicious node. Mainly the malicious node will give fast route reply with high destination sequence number Moreover on identifying the malicious node the routing table and messages from malicious node are not forwarded in network. Our proposed algorithm has shown great improvement in Hop count, execution time and throughput. The proposed solution does not require any type of overhead on destination node or any intermediate node on AODV routing protocol. We have also used fuzzy IF-THEN rules to identify and delete attacks. The fuzzy rule is implemented by using response time from node. The algorithm will provide better solution for reduction of data loss over network.

Fuzzy logic is a rule based approach for solving the problem rather than automating the model. The proposed system will improve the performance of MANET under attack. The results have shown that proposed system has better performance than classic AODV in all its parameters like execution time, throughput, hop count etc. Our system not only detects the attack but also isolates it from network thereby improving the performance to great level.

The future scope of work is that the proposed security mechanism may be extended to defend against other attacks like grey hole attack, packet dropping attack, resource consumption attack. In order to detect attacks, various fuzzy rules can be generated by applying neuron fuzzy application.

Surface Diagram (Lateral View)



X (input): Seq
Y (input): RespTime
Z (output): output
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101

Figure 14: Surface diagram displaying the no of malicious nodes (Lateral view)

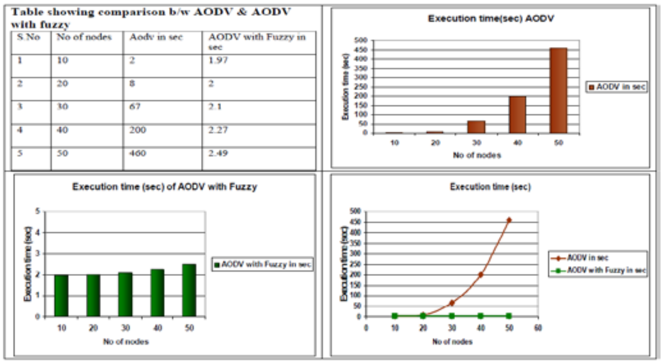


Table showing comparison b/w AODV & AODV with fuzzy

S.No	No of nodes	Aodv in sec	AODV with Fuzzy in sec
1	10	2	1.97
2	20	8	2
3	30	67	2.1
4	40	200	2.27
5	50	460	2.49

Figure 15: Graph showing the execution time (sec) of AODV & AODV with fuzzy logic

No of nodes	Round	Malicious count	Rate	Rate*2500
100	10	3	3.00%	7500
200	20	3	2.00%	5000
300	30	6	2.00%	5000
400	40	7	1.75%	4375
500	50	9	1.80%	4500

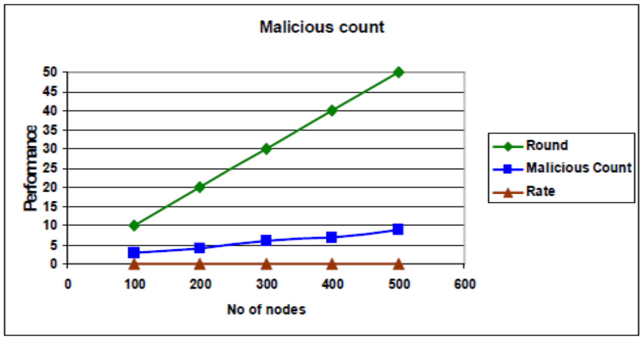


Figure 16: Graph showing malicious count & rate% of AODV & AODV with fuzzy

8.0 ACKNOWLEDGEMENT

I would like to thank the institution who helped a lot in this study. Also, special thanks to my guide and co-guide in sparing their time providing their valuable inputs as and when required during the course. Many thanks to all the peers, colleagues and organizations who supported this research by sharing their valuable time and feedback on their experiences in application of Fuzzy logic in Intruder Detection System.

9.0 REFERENCES

[1]. Adhoc & Sensor Network by Carloss De Morais, ISBN-981-256-681-3 Pg [1] [2].

[2]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor net-works: a survey. Computer Networks, 38(4):393–427, 2002.

[3]. Dong Seong Kim, Khaja Mohammad Shazzad, and Jong Sou Park. A framework of survivability model for wireless sensor network. IEEE Proceedings of the First Interna-tional Conference on Availability, Reliability and Security, February 2006.

[4]. Boole G., "The Laws of Thought", New York: Dover Books (Reprinted), 1958.

[5]. Zadeh, L. A., "From Circuit Theory To Systems Theory", Proceedings of the Institute of Radio Engineering, Vol.50, 1962.

[6]. Zadeh, L. A., "Fuzzy Sets", Information And Control, Vol. 8, 1965

[7]. Antonio M. Ortiz and Teresa Olivares: Fuzzy Logic Applied to Decision Making in Wireless Sensor Networks, Fuzzy Logic – Emerging Technologies and Applications ISBN 978-953-51-0337-0

[8]. B.Ben Sujitha1, R.Roja Ramani2, Parameswari: Intrusion Detection System using Fuzzy Genetic Approach; International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 10, December 2012

[9]. Sampada Chavan, Neha Dave and Sanghamitra Mukherjee"Adaptive Neuro-Fuzzy Intrusion Detection Systems" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 $ 20.00 © 2004 IEEE

[10]. Bharanidharan Shanmugam and Norbik Bashah Idris."Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks" 2009 International Conference of Soft Computing and Pattern Recognition

[11]. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park "Black Hole Attack in Mobile Ad Hoc Networks" ACM SouthEast Regional Conference 2004.

[12]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[13]. X. Wang, T. Lin and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, 2005.

[14]. N.H.Mistry, D. C. Jinwala, M. A. Zaveri. "Prevention of Blackhole Attack in MANETs". In: Proceedings of EPWIE-2009, Gujarat, India, pp.89-94, July 2009.

[15]. Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc On-Demand Distance Vector Routing." In: Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90–100, February 1999.

[16]. Latha Tamilselvan, V Sankaranarayanan. "Prevention of Blackhole Attacks in MANET." In: Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.

[17]. M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.

[18]. Elmar Gerhards-Padilla," Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks 0742-1303/07© 2007 IEEE.

[19]. Devendra K. Tayal, Amita Jain and Vinita Gupta "Fuzzy Expert System for Noise Induced Sleep Disturbance and Health Effects" in BIJIT Issue3: (Jan-June 2010 Vol2 No1)

[20]. Zaheeruddin, Vinod K. Jain, and Guru V. Singh , "A Fuzzy Model For Noise-Induced Annoyance", IEEE transactions on systems, man, and cybernetics –Part A: Systems and Humans, Vol. 36(No. 4), July 2006.