Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET

Kulbhushan
Asst. Prof,Department of
Electronics & Communication
Engg., GTBKIET,Malout

Jagpreet Singh
Research Scholar,Department
of Computer Science & Engg.,
IIT Ropar

ABSTRACT

Security[16] is an essential feature for wired and wireless network[1]. But due to its unique characteristics of MANETs[10], it creates a number of consequential security challenges to network. MANETs are vulnerable to various attacks[2], blackhole[12] is one of the possible attack. In this paper, we represent an intrusion detection[5] system for MANETs against blackhole attack using fuzzy logic[4]. Our system successfully detects the blackhole in the network and this information is passed to other nodes also. We also provide a detailed performance evaluation based on various network parameters. Our results show that the proposed system not only detects the blackhole[12] node, but improves the performance of AODV under the blackhole attack.

General Terms

Computer Network, Wireless Network, Manets, Security Issues.

Keywords

MANET, AODV, Blackhole Attack, Fuzzy Logic.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET)[10] is an infrastructure less, multi hop network, in which mobile nodes communicate directly or co-operatively with each other. As there are no access points or routers, no co-ordination or configuration prior to setup of a MANET is required. Also, due to high mobility, resource constrains (power, storage and bandwidth) in MANET environment, and nodes operating in a dynamic topology, more challenges are encountered in routing.

The Ad-hoc on demand distance vector (AODV)[3][9] routing protocol[15] is designed for use in MANETs. AODV is a reactive protocol i.e. the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up to date and to prevent routing loops. An important feature of AODV[3] is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

Wireless Ad-hoc networks are vulnerable to various attacks[2]. These include passive eavesdropping, active interfering, impersonation and denial of services. One of these attacks is blackhole attack. In blackhole attack, node will pretend as if it is a destination node for a particular route and absorbs all data packets in itself, similar to a hole that sucks everything in. In this way, all packets in a network are dropped. A malicious node dropping all traffic in a network makes use of vulnerabilities of the route discovery packets of the on demand protocols, such as AODV.

In this paper, we have proposed a novel method based on fuzzy logic[4] to detect blackhole[12] attack. The system isolates the blackhole node from the network. The proposed solution is used by every node in the network. So, every node in the network can determine the behavior of its neighbors, if neighbor is malicious, an alarm packet is broadcasted in the network with the IP address of malicious node and that node thereafter is not allowed to participate in packet forwarding operation.

Following is an overview of this paper: in section 2, we describe our fuzzy based intrusion detection system and its implemented features. In section 3, the results of simulation are discussed and finally the conclusions are summarized in section 4.

2. PROPOSED SYSTEM

The proposed system is based upon fuzzy logic[4][14]. Fuzzy logic is a form of multi valued logic derived from fuzzy set theory to deal with reasoning that is approximate rather than precise. In contrast with "crisp logic", where binary sets have binary logic, fuzzy logic variables may have a truth value that ranges between 0 and 1 and is not constrained to the truth values of classic propositional logic.

The fuzzy model[6] is integrated with AODV[3][9] routing protocol as shown in figure 1. It consists of following four components namely Fuzzy Parameter Extraction, Fuzzy Computation, Fuzzy Verification Module and Alarm Packet Generation Module. During fuzzy parameter extraction, the system extracts the parameters required for analysis from network traffic. These parameters are passed to fuzzy computation module, which applies various fuzzy rules and membership functions to calculate fidelity level of the node. This fidelity level is compared with threshold value in fuzzy verification module to check the behavior of node and if, fidelity level is less than threshold level, an alarm packet with the IP address of detected malicious node is broadcasted in the network.

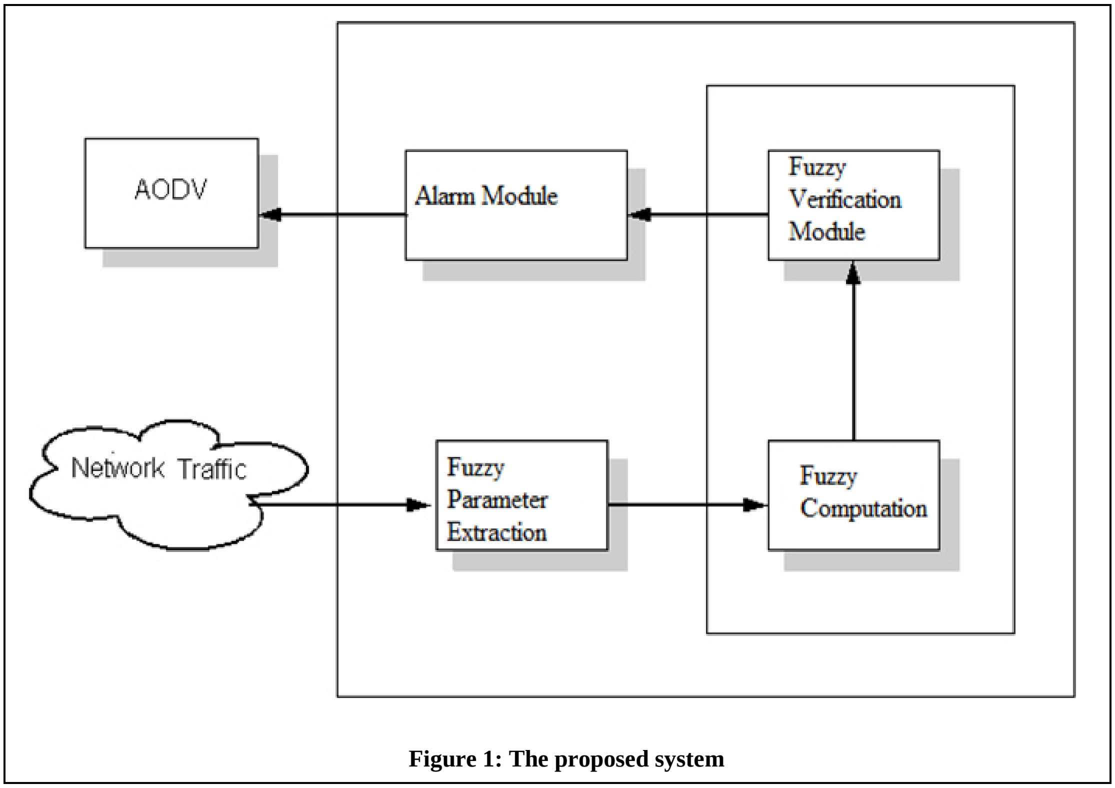

Figure 1: The proposed system

2.1 Fuzzy Parameter Extraction

The input to the fuzzy system in node " i " is extracted by listening to the traffic received and generated by its immediate neighbors and creates a fuzzy parameter list in new neighbor table for its every neighbor. Each node in the network works in the promiscuous mode (i.e. it can listen to the traffic of its neighbors) and listens to the routing and network traffic of their neighbors and collects the information for fuzzy system. The neighbor table of node " i " has the following fields for its neighbor node " j " : Forward Packet Ratio, Average Destination Sequence Number and Fidelity Level.

Forward Packet Ratio : If a route has been established through node j, node I in its immediate neighborhood will listen to the traffic through node j. If node j is not the destination, it must forward every data packet it is receiving from its neighbor in the route. So the neighboring nodes of node j will activate their promissious mode and will listen to the traffic through node j and calculate the forward packet ratio.

Forward packet ratio : data packets forwarded / data packets received

Average Destination Sequence Number : In RREP packet of AODV, destination transmits its updated sequence number. The sequence number of a particular node depends upon the number of connections of respective node in the network. A node having high value of destination sequence number is assumed to be a reliable node in AODV. A malicious node in the network will show high value of its destination sequence number[11][13] to pretend as a destination. So, if a node is blackhole node, it will transmit highest destination sequence number and pretends to be the destination. So, we can check the behavior of node according to the sequence number. To check out the variations in the sequence number, we are calculating the average of the difference of destination sequence number[11][13] in each time slot between the previous sequence number in the neighbor list and RREP packet. The time interval to update the Average Destination Sequence Number is as soon as a node transmits a RREP packet.

2.2 Fuzzy Computation

The proposed system receives forward packet ratio and average destination sequence number as input from routing and network traffic and has one output, Fidelity Level. The rule bases[14] for the evaluator is shown in table 1. The membership functions[14] are drawn for all inputs and output of fuzzy system. The bases of functions are chosen so that they result in optimal value of performance measures. To illustrate one rule, the first rule can be interpreted as " If forward packet ratio is LOW and sequence number ratio is LOW, then fidelity level is LOW". Similarly, the pther rules are framed based on Mamdani fuzzy model, each node computes the fidelity level for its neighbors according to the membership functions developed for the input and output variables as as shown in figure 2 and maintained in the neighbor table. The fidelity level lies between 0 and 10. The minimum value for fidelity can occur as a result of more malicious behavior than legitimate behavior of a neighboring node. Hence, a fidelity level of 0 represents complete malicious behavior and 10 represents legitimate behavior of a particular node.

2.3 Fuzzy Verification Module

In the verification module, the calculated fidelity level is compared with the threshold fidelity level, which is set at 5.5. If the computed fidelity level is less than threshold level, the node is blackhole node, otherwise node is legitimate node.

Table 1. Fuzzy Rule Base

S.N.	Forward Packet Ratio	Average Destination Sequence Number	Fidelity Level
1.	LOW	LOW	LOW
2.	LOW	MEDIUM	LOW
3.	LOW	HIGH	LOW
4.	MEDIUM	LOW	MEDIUM
5.	MEDIUM	MEDIUM	MEDIUM
6.	MEDIUM	HIGH	LOW
7.	HIGH	LOW	HIGH
8.	HIGH	MEDIUM	HIGH
9.	HIGH	HIGH	LOW

2.4 Alarm Packet

On the basis of information passed by fuzzy verification module, if the fidelity level is less than the threshold fidelity level, this model generates an alarm packet with IP address of the node, that is declared as blackhole node. So the blackhole node is isolated from the network.

3. EVALUATION OF THE SYSTEM

3.1 Parameters Chosen for Evaluation

A number of intrusion detection schemes[2] for MANETs[10] have been suggested and they all try to detect the intrusions in the network using the different aspects of routing protocols and of network. But how it is decided, which one is best. This depends upon structure and properties of the network. The nodes might be moving fast or slow, they might be highly concentrated into a small area or widely spread out over a large area. There are many questions that a designer of a system has to take into account. It is necessary to choose suitable metrices for system evaluation. The performance metrices describes the outcome of the simulation or set of simulations. These metrices are interesting because they can be used to point out what really happened during the simulation and provide valuable information about the proposed system. The following metrices are chosen in this work for system evaluation.

3.1.1 Detection Rate

It is the rate of detecting the blackhole node in the network.

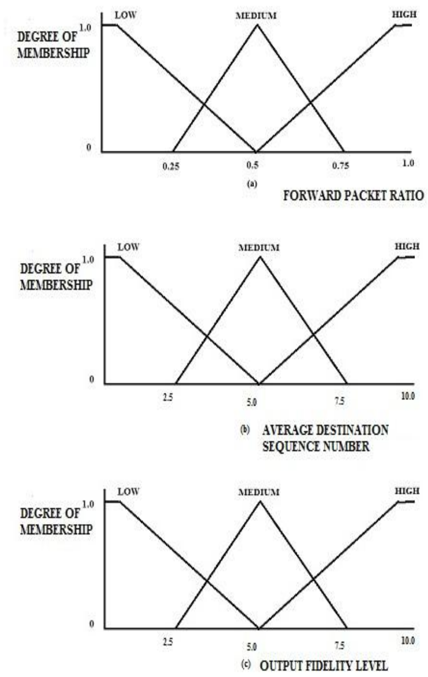

Figure 2 : Membership Functions for Fuzzy System

It is very important metric as it signifies the success of intrusion detection system.

3.1.2 False Positive Alarm

It is the number of times, a legitimate node is detected as malicious node.

3.1.3 Packet Delivery Ratio

The ratio between the number of packets originated by the application layer at CBR source and the number of packets received by application layer at CBR sink at final destination. It is desirable that a routing protocol keeps this ratio high. The greater this ratio is, the reliable the adhoc network will be.

Packet Delivery Ratio = Received packets / Sent packets

Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput that the network can support. This metric characterizes both the completeness and correctness of the routing protocol.

3.1.4 Routing Overhead

The total number of routing packets transmitted & received by all the nodes during the simulation known as routing overhead as energy dissipates both in sending a packet as well as receiving a packet for processing it. For packets sent over multiple hops, each transmission of the packet counts as one. This is interesting metric. In some way it reveals how bandwidth efficient the routing protocol is. The routing overhead metric simply shows how much of the bandwidth (which often is one of the limited factors in a wireless system) that is consumed by routing messages, i.e. the amount of bandwidth available to data packets. The routing overhead is typically much larger for proactive protocols since it periodically floods the network with updates messages. As the mobility in the network increases, reactive protocols will of course have to send more and more routing messages. This is where the real strengths and weaknesses of the routing protocol revealed. It is an important metric for comparing protocols, as it measures the scalability of a protocol, the degree to which it will function in congested or low-bandwidth environments.

3.1.5 End to End Delay

End-to-End Delay is average time a packet takes for delivery to its destination after it was transmitted. It tells how a protocol adapts or arranges for an immediate delivery of packets to its desired destination.

3.2 Simulation Parameters

Various default parameters like Channel, Propagation medium, Network Interface type, MAC protocol, Link layer type, interface queue, antenna type are same for both scenarios. Other default parameters like path of node-movement file and traffic-generation file are needed to mention accordingly in the tcl script file. The simulation parameters used to produce the simulation suite for this work are presented and explained as follows:

Table 2: Summary of common Parameter used in Simulation

Parameters	**Value**
Simulator	Ns-2(2.29)
Routing Protocol	AODV
Transmitter Range	250 m
Bandwidth	2Mbits/s
Simulation Time	200
Number of nodes	50
Scenario size	1000 x 1000 m2
Traffic type	Constant Bit Rate
Packet size	64 bytes
Rate	4 packets/s

A scenario size is chosen as 1000m x 1000 m square because square area does not discriminate one direction of motion like rectangular area do. The transmitter range of IEEE 802.11 nodes in ns-2[7] is 250m [9] and this is maximum possible distance between two mobile nodes. They cannot communicate with each other beyond this. The source-destination pairs are spread randomly over the network. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network. Traffic sources are CBR (continuous bit-rate). Each node starts its journey from a random location to a random destination according to the speed parameter specified in the scenarios. All the simulation parameters are shown in table 2.

3.3 Scenario-1:Varying mobility of nodes

In Scenario-1,AODV[3][9] is tested in proposed system for different mobility of nodes and rest of parameters remains constant. And speed is varied from constant 10m/s to 70m/s. This is a very interesting analysis scenario as it shows the performance in terms of nodes mobility. More the mobility, more the link breaks will be and both the protocols can be tested to depth. Again analysis is done using all five parameters.

3.3.1 Detection Rate

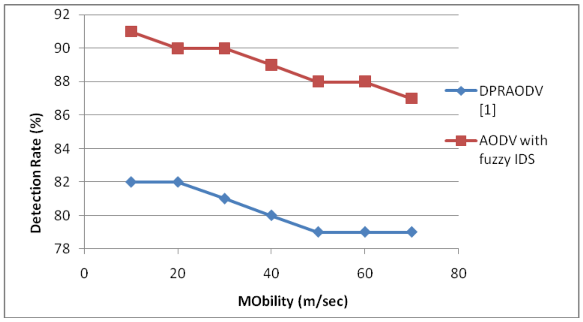

Figure 3:Detection Rate Senario-1

3.3.2 False Positive Alarm

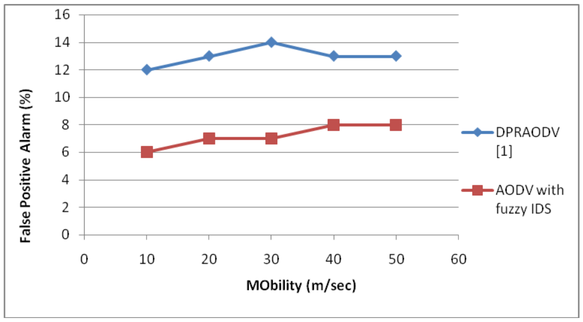

Figure 4: False Positive Alarm Senario-1

3.3.3 Packet Delivery Ratio

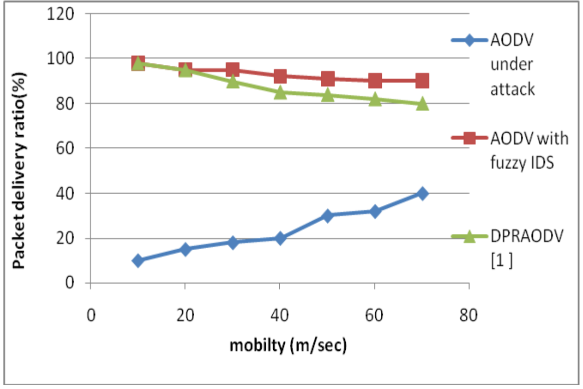

Figure 5: Packet Delivery Ratio Senario-1

3.3.4 Average End to End Delay

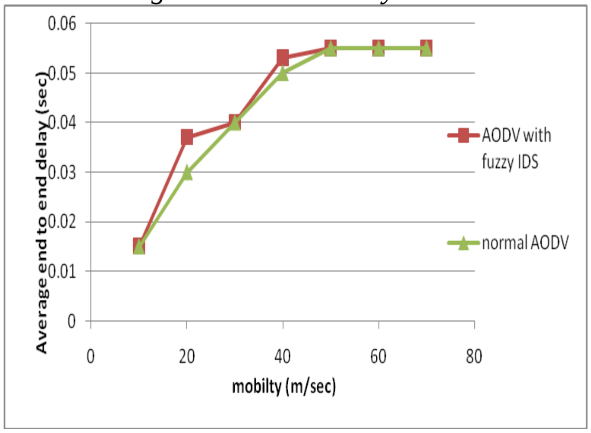

Figure 6:Average End to End Delay Senario-1

3.3.5 Normalized Routing Overhead

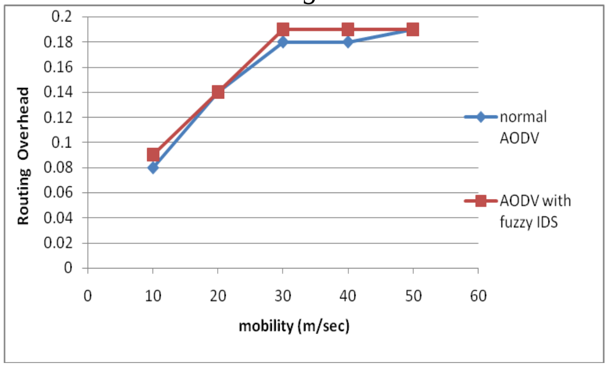

Figure 7: Normalized Routing Overhead Senario-1

3.4 Scenario-2:Varying Network Size

In Scenario-2, simulation is done for different number of nodes in the network and rest of parameters remain constant. Following section discusses results after simulation.

3.4.1 Detection Rate

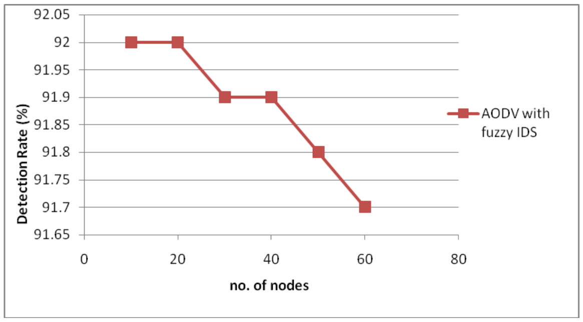

Figure 8: Detection Rate Senario-2

3.4.2 False Positive Alarm

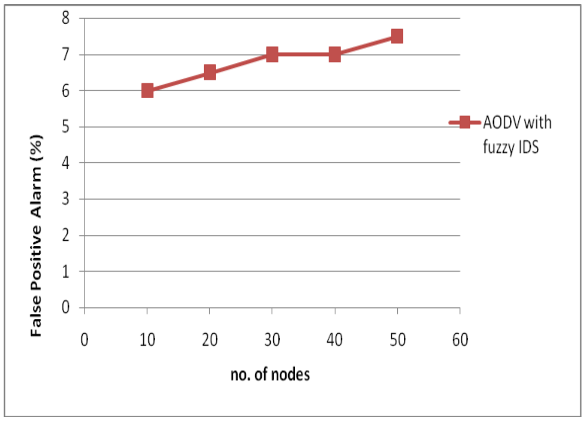

Figure 9: False Positive Alarm Senario-2

3.4.3 Packet Delivery Ratio

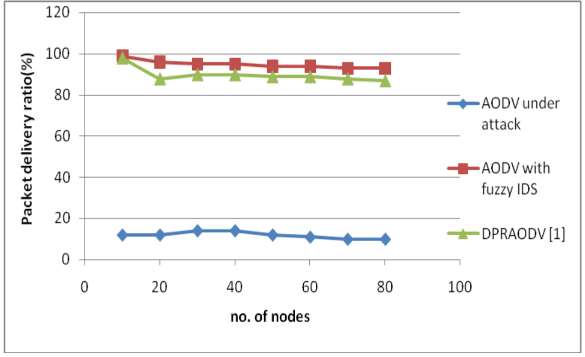

Figure 10: Packet Delivery Ratio Senario-2

3.4.4 Average End to End Delay

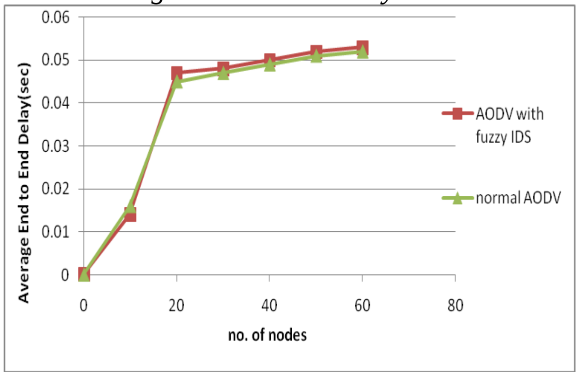

Figure 11:Average End to End Delay Senario-2

3.4.5 Normalized Routing Overhead

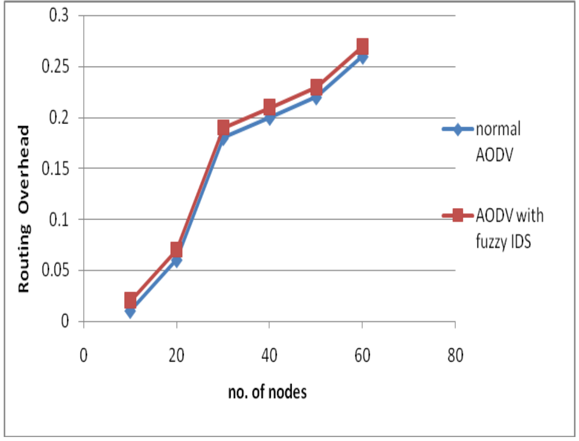

Figure 12:Normalized Routing Overhead Senario-2

3.5 Scenario-3:Varying Network Size

In Scenario-3, simulation is done for different number of sources in the network and rest of parameters remain constant. Following section discusses results after simulation.

3.5.1 Detection Rate

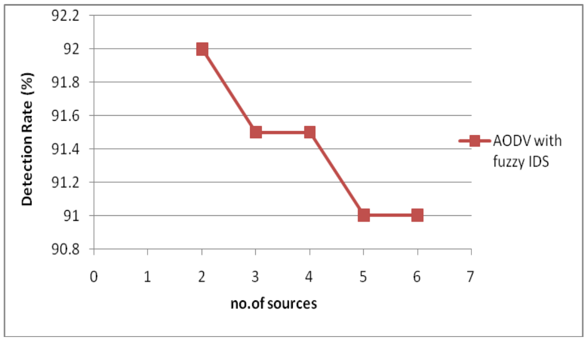

Figure 13: Detection Rate Senario-3

3.5.2 False Positive Alarm

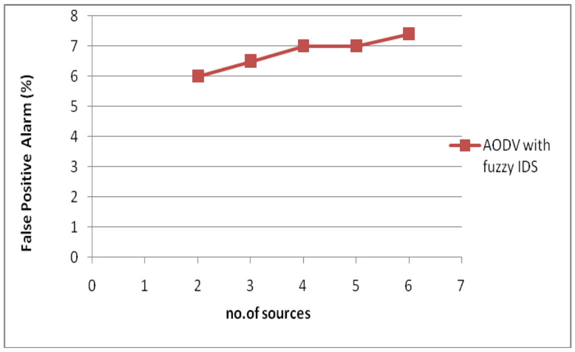

Figure 14: False Positive Alarm Senario-3

3.5.3 Packet Delivery Ratio

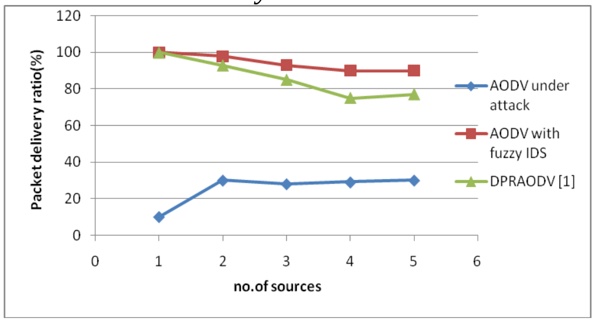

Figure 15: Packet Delivery Ratio Senario-3

3.5.4 Average End to End Delay

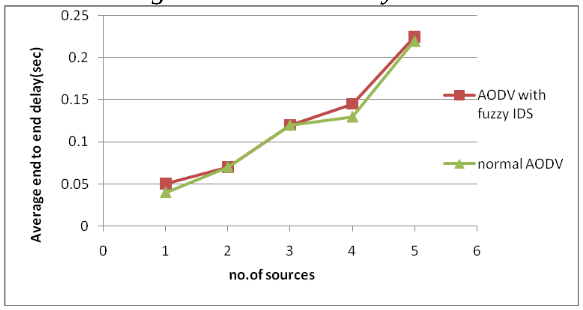

Figure 16:Average End to End Delay Senario-3

3.5.5 Normalized Routing Overhead

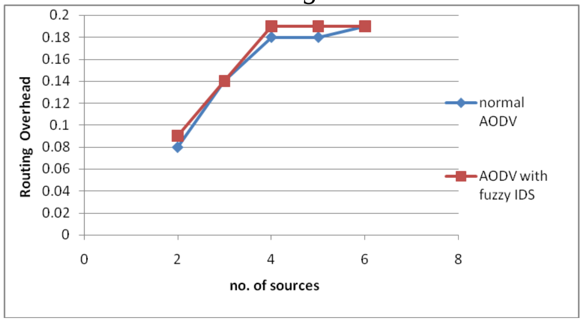

Figure 17:Normalized Routing Overhead Senario-3

3.6 False Detection Rate v/s Threshold Fidelity Level

We had also find out false detection rate as compared with threshold fidelity level. If the threshold level in fuzzy system is kept at low values, the successful detection of malicious behavior decreases and chances of considering malicious nodes as legitimate node increases. But if threshold is kept at very high value, the legitimate nodes are also considered as malicious, thus again increasing the false detection rate. As shown in figure 6.16, the most suitable value of threshold is between 5 -5.5.

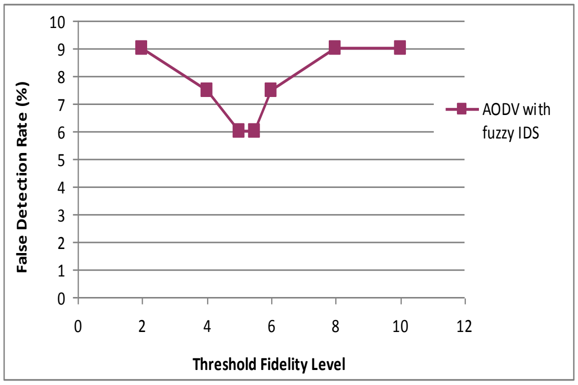

Figure 18: False Detection v/s Yhreshold Fidelity Level

4. CONCLUSION

In this proposed system, we have provided fuzzy logic based a very simple and effective solution to detect and isolate the blackhole node from AODV enabled MANET[10]. Fuzzy logic[4][14] incorporates a simple, rule based approach to solving a problem rather than attempting to model a system automatically. As we know the performance of network falls to a very low value under the blackhole attack. As illustrated by result graphs, the performance of MANET under blackhole attack improves significantly, when the proposed system is used. The Results in different scenarios prove that proposed system performs better than classic AODV in all of the parameters like routing overhead, end to end delay, packet delivery ratio. Our system not only detects the blackhole attack in early stage of communication, but isolates it from the network. Thus improving the performance to great level.

5. ACKNOWLEDGEMENTS

Our thanks to the experts those have contributed towards development of the fuzzy based intrusion detection system. The constant guidance and encouragement received from Mr. Sukhdev Singh, head of department ECE in GTBKIET,Malout has been an immense help in carrying out the present work and is acknowledged with reverential thanks.

6. REFERENCES

[1] Andrew S Tanenbaum " Computer Networks " Prentice Hall of India, third edition.

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei," A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks " Department of Computer Science and Engineering, Florida Atlantic University

[3] C. Perkins, E Belding-Royer,(July 2003) "Ad hoc On-demand Distance Vector (AODV)" Request For Comments (RFC) 3561.

[4] Fuzzy Logic with Engineering Applications by Timothy J.Ross Mcgraw Hill, Inc.

[5] I. Stamouli, P. G. Argyroudis and H. Tewari, (2005) "Real-time intrusion detection for ad hoc Networks", Sixth IEEE Intl Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), pp.374-380.

[6] J. Martin Leo Manickam Anna and S.Shanmugavel (2007)," Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET ",third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob2007).

[7] Kevin Falland Kannan Varadhan, (April, 2005)"NS-Documentation, http://www.isi.edu/nsnam/ns/ns-documentation.html".

[8] M. Hollick, J. Schmitt, C. Seipl and R.Steinmetz,(June 2004) "On the effect of node misbehavior in ad hoc networks", Proc. Of IEEE Intl Conference on Communications (ICC'04), Paris, pp. 3759-3763.

[9] M. Hollick, J. Schmitt, C.Seipl and R.Steinmetz, (Feb 2004) "The ad hoc on- demand distance vector protocol: an analytical model of the route acquisition process", Proc. of Second Intl Conference on Wired/Wireless Internet Communications (WWIC'04), Frankfurt, pp. 201-212.

[10] MANET Charter,(1998) available at http://www.ietf.org/html.charters/manet -charter html (1998-11-29).

[11] Payal N. Raj and Prashant B. Swadesh (2009) "DPRAODV: A Dynamic Learning System against Blackhole attack in AODV based MANET ", International Journal of Computer Science, Vol. 2.

[12] R.A. Raja Mahmood, A.I. Khan (2007) "A Survey on Detecting Black Hole Attack in AODV- based Mobile Ad Hoc Networks ",Clayton School of information Technology, Monash UniversityAustralia High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on

[13] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto (Nov. 2007) "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,

[14] Timothy J. Ross,(I2000)"Fuzzy Logic with Engineering Applications",McGraw Hill International Editions, International Editions.

[15] Tony Larsson and Nicklas Hedman (1998) "Routing Protocols in Wireless Ad-hoc Networks – A Simulation Study ", Lulea University of Technology , Stockholm

[16] V. Karpijoki,(2000) "Security in Ad hoc Networks", In Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland.

[17] Y.Zhang, W. Lee, and Y. Huang,(September 2003) "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5.

[18] Y. Zhang, W. Lee,(August,2000) "Intrusion Detection on Wireless Ad hoc Networks", in Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00).