ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network

J.Ramkumar[#1], R.Murugeswari[#2]

[#1]Post Graduate Student, Department of Computer Science and Engineering, Kalasalingam University, Tamilnadu, India

[#2]Assistant Professor, Department of Computer Science and Engineering, Kalasalingam University, Tamilnadu, India

ABSTRACT-- Security is one of the main issues in WMN and this network is exposed to various attacks, black hole is one of the possible attacks. The black hole attack is a type of denial-of-service attack which passed out disrupts the service of network layer. In our project, we have proposed on fuzzy logic scheme to detect black hole attack and improve the performance of AODV in the parameters like end to end delay, packet delivery ratio. Fuzzy is a mathematical logic that attempts to solve problems by assigning values to an imprecise spectrum of data in order to reach the most accurate conclusion possible.

KEYWORDS-- WMN, AODV, Black hole attack, Fuzzy logic.

I. INTRODUCTION

Wireless Mesh Networks (WMNs) are build on a mix of fixed and mobile nodes interconnected by the use of wireless links to form a multi-hop ad hoc network. [1] Wireless mesh networks consist of mesh routers and mesh clients, where mesh routers have smallest mobility and form the backbone of WMNs. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers. Infrastructure WMN may provides connectivity to other networks such as internet, wifi, wimax, etc. Mesh clients can contact the network through MR as well as directly meshing with other mesh clients. A Hybrid WMN combines the connectivity [22] model of both the Infrastructure and Client WMNs. In these networks, both the Mesh Clients and Mesh Routers are aggressively involved in the routing and forwarding of packets. The Ad hoc On Demand Distance Vector (AODV) [18] routing algorithm is a routing protocol considered for ad hoc mobile networks. AODV maintains these routes as long as they are necessary by the sources. When a source node needs a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. And the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

In a black hole attack, [16] the malicious node always replies positively to a Route Request although it may not have a valid route to the destination. Since the malicious node does not check its routing entries, it will always be the first to reply the Route Request message. [9] Therefore, almost all the traffic within the neighborhood of the malicious node will be directed towards the malicious node which may drop all the packets resulting in denial of service.

Fuzzy logic builds on a set of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. In this paper, we design a fuzzy logic system to detect the black hole in wireless mesh network. [14] This simplifies the job of the system designer and the computer, and results in much more accurate representations of the way systems behave in the real world. Additional benefits of fuzzy logic include its simplicity and its flexibility. Fuzzy logic can handle problems with inaccurate and incomplete data, and it can model nonlinear functions of arbitrary complexity.

II. RELATED WORK

Sukant et al.,[12] described the malicious attack performance of the network almost completely which may not forward any traffic at all to neighbor node. Detection of malicious node and isolation of malicious node will stop sending fake request call. It has been made to find impact of malicious node in AODV routing protocol under different density of node with number of malicious attack, that throughput and packet delivery ratio of normal AODV is much better than AODV with malicious attack. **A.Valarmozhi et al.[1]** proposed on existing MAC, routing, and transport protocols, network performance was not scalable with either the number of nodes or the number of hops in the network. The problem can be alleviated by increasing the network capacity through using multiple channels/radios per node or developing wireless radios with higher transmission speed. **Asma Begam et al.,[9]** discussed a lightweight, fast, efficient and mobile agent technology based security solution against black attack for wireless sensor networks. The proposed scheme is to defend against black hole attack using multiple base stations deployed in network by using mobile agents. **Gayatri et al.,[13]** described the defense algorithm to detect the selective forwarding attack. It considers a more challenging scenario that the intentional selective dropping may be interleaved with normal loss events due to channel quality or medium access collision. Novel algorithm can efficiently transfer the packet from source to destination using fuzzy theory and can detect the attacker effectively using more challenging scenario. **Kulbhushan et al.,[5]** proposed the fuzzy logic based a very simple and effective solution to detect and isolate the black hole node from AODV enabled MANET. Fuzzy logic incorporates a simple, rule based approach to solving a problem rather than attempting to model a system automatically. The performance of network falls to a very low value under the black hole attack. The fuzzy system is used the performance of MANET under black hole attack improves significantly. **Yaser et al.,[7]** discussed one of the security problems in ad hoc networks called the black hole problem. Trust table protocol modifies the behavior of the original AODV to check the reliability of the received routes before sending the data packets. The protocol reduces the bad affects of the black hole problem and outperforms the original AODV in terms of packet delivery ratio, number of dropped packets, end-to-end delay, and overhead the protocol does not consider the behavior of two black hole nodes working together as a team. **Akanksha et al.,[8]** discussed the collection of mobile nodes that dynamically form a temporary network and are infrastructure less. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The damage will be serious if malicious nodes work together as a group. Our protocol not only prevents black hole but also improves performance. **Yuste et al.,[11]** proposed a technique by which the dimension of this area and the periodicity of the Gateway advertisements are controlled. The fuzzy system takes into account the number of link changes, the movement of the traffic sources and the number of solicitations that the sources generate. The system shows the goodness of our proposal in terms of packet loss rate and normalized overhead. **Payal et al.,[4]** described a very simple and effective way of providing security in AODV against black hole attack. Our prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbors. **Sankaranarayanan et al.,[3]** proposed the routing security issues of MANETs. One type of attack, the black hole, which can easily be deployed against the MANET is described and a feasible solution for it by making use of ‘fidelity tables’ and assigning fidelity levels to the participating nodes. The percentage of packets received through our system was better than that in AODV in presence of cooperative black hole attack.

III. PROPOSED SYSTEM

The proposed system is based on fuzzy logic. It 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", [14] 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. Using Mamdani fuzzy module,

R_i : if $x\tilde{}$ is A_i then $y\tilde{}$ is B_i. i=1,2,……,k

Here

$x\tilde{}$ → input (antecedent) linguistic variable,

A_i → antecedent linguistic terms (constants),

$y\tilde{}$ → output (consequent) linguistic variable,

B_i → consequent linguistic terms.

The fuzzy mode is integrated with AODV routing protocol. It consists of following four components namely fuzzy factor withdrawal, Fuzzy calculation, Fuzzy confirmation Module and Alarm Packet Generation Module. The fuzzy factor withdrawal is used to the system that extracts the parameters required for analysis from network traffic. And these requirements are passed to fuzzy calculation module, which applies various fuzzy rules and membership functions to calculate [3] fidelity level of the node. This fidelity level is compared with threshold value in fuzzy confirmation module to check the behavior of node and the fidelity level is less than threshold level, an alarm packet with the IP address of detected malicious node is broadcasted in the network.

A.Fuzzy Factor Withdrawal

The input to the fuzzy system in node "a" is extracted by listening to the traffic received and generated by its immediate neighbors. Each node in the network can listen to the traffic of its neighbors and listens to the routing and [5] network traffic of their neighbors and collects the information for fuzzy system. The neighbor table of node "a" has the following fields for its neighbor node "b" Forward Packet Ratio, Average Destination Sequence Number and Fidelity Level.

Forward Packet Ratio: If a route has been established through node b, node a in its immediate neighborhood will listen to the traffic through node b. So the neighboring nodes of node b will activate their loose mode and will listen to the traffic through node b and calculate the forward packet ratio.

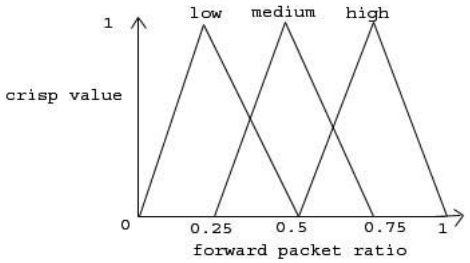

Fig 1: Forward Packet Ratio

Forward packet ratio: data packets forwarded / data packets received

Average Destination Sequence Number: The sequence number of a node depends upon the number of connections of respective node in the network. A node have high value of destination sequence number is assumed to be a reliable node in AODV.

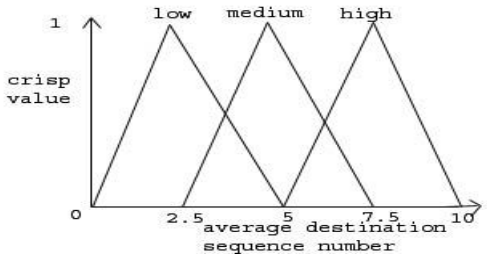

Fig 2: Average Destination Sequence Number

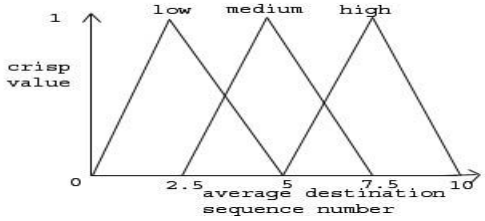

Fig 2: Average Destination Sequence Number

A malicious node in the network will show high value of its destination sequence number to act as a destination. So, we can check the behavior of node according to the [20] sequence number. To check out the variations in the sequence number, we are calculating the average of the difference of destination sequence number 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.

B.Fuzzy Calculation

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 represent below Fig 3. The membership functions are drawn for all inputs and output of [11] fuzzy system. The bases of functions are chosen so that they result in optimal value of performance measures.

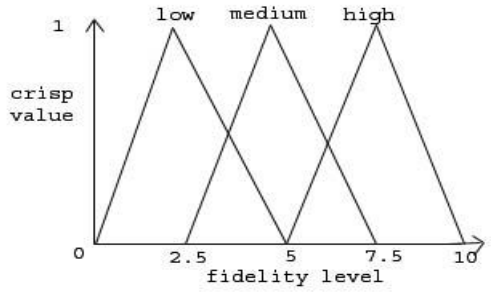

Fig 3: Fidelity Level

To illustrate one rule, the first rule can be interpreted as "If X is LOW and Y is LOW, then Z is also LOW". Similarly, the other 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 are maintained in the neighbor table. The fidelity level lies between 0 and 10. [17] The minimum value for fidelity can occur as a result of more malicious behavior than genuine behavior of a neighboring node. Hence, Fidelity level of 0 →complete malicious behaviors and 10 → genuine behavior of a particular node.

C.Fuzzy Confirmation Module

In the confirmation module, the calculated fidelity level is compared with the threshold fidelity level, which is set at 6. If the computed fidelity level is less than threshold level, the node is black hole node, otherwise node is legitimate node.

D.Alarm Packet

On the basis of information passed by fuzzy confirmation module, if the fidelity level is less than the threshold fidelity level, this model generates an alarm packet with IP address of the node, which is confirmed as black hole node. So the black hole node is isolated from the network.

IV SIMULATION PARAMETER

The simulation parameters used to produce the simulation suite for this work are presented and explained as follows:

TABLE I

Parameters	**Values**
Simulator	NS 2.35
Routing Protocol	AODV
Number of nodes	20
Simulation time	600 ms
Number of topologies	10
Traffic type	Constant Bit Rate
Scenario Size	900 X 850
Bandwidth	1 Mbps
Packet Size	64 Bytes

In our project ns-2.35 network simulator was used, the scenario size is set to be 900X850. The Routing protocol is used in the network called AODV. The packet size is used in the network are 64 bytes. We calculate the parameter like packet delivery ratio and end to end delay are calculated by using the trace file.

V. EXPRIMENTAL RESULT

A.Packet Delivery Ratio

In our parameter, while the packet delivery ratio is decrease in black hole AODV when compare to the normal AODV. In our system there was 20% of malicious node occur in the black hole. PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source.

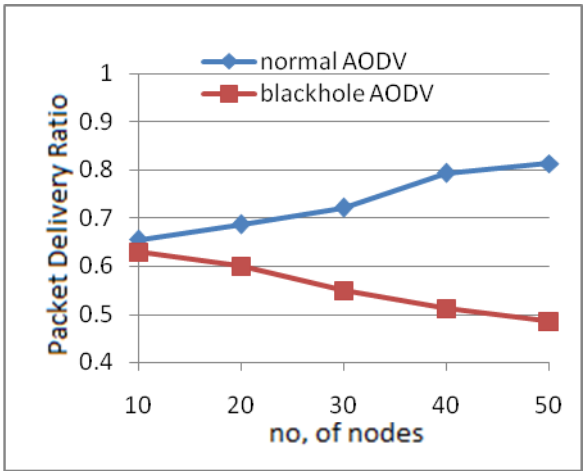

Fig 4: Packet Delivery Ratio

The above fig 4 depicts the difference between normal and black hole node with respect to packet delivery ratio. The result shows the Black hole AODV of packet delivery ratio is decrease while compare to the normal AODV.

B.End to End Delay

The average delay between sending of the data packet by CBR source and its receipt at the corresponding CBR receiver.

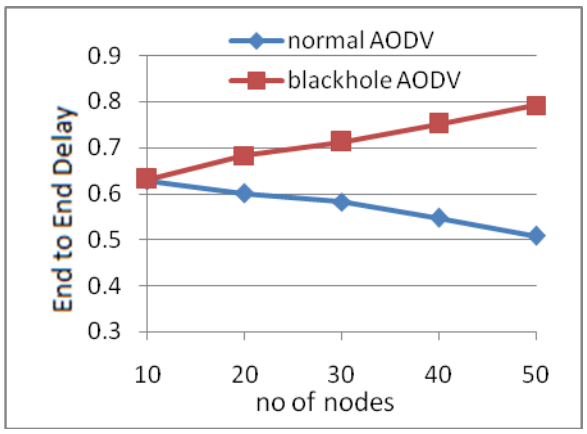

Fig 5: End to End Delay

The above fig 5 shows the difference between normal and black hole node with respect to End to End delay. The delay is increased in black hole AODV when compare to the normal AODV.

VI. CONCLUSION

In this paper, we analyze the problem of black hole attacks in AODV routing protocol in mesh network. We proposed a fuzzy system to detect the black hole attack on the AODV protocol. We simulated our proposed solution using the NS-2.35 simulator and compared the performance in terms of packet delivery ratio and delay. Our simulation results show that, greatly suffers from black holes in terms of packet delivery ratio and delay. Our system not only detects the black hole attack and also isolates black hole from the network.

REFERENCES

[1]. A.Valarmozhi, M.Subala, V.Muthu "Survey of Wireless Mesh Network" *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 2, Issue 6, December 2012.

[2]. Om Shree, Francis J. Ogwu, "A Proposal for Mitigating Multiple Black Hole Attack in Wireless Mesh networks", *(http://www.scirp.org/journal/wsn* Wireless Sensor Network, 2013

[3]. Latha Tamilselvan, Dr. V.Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

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

[5]. Kulbhushan, Jagpreet Singh, "Fuzzy logic based intrusion detection system against black hole attack on AODV in MANET". *IJCA Special Issue on Network Security and Cryptography NSC, 2011*

[6]. Mihail L. Sichitiu "Wireless Mesh Networks: Opportunities and Challenges".

[7]. Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein," A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks" *International Journal of Communication Networks and Information Security (IJCNIS)*,2011

[8]. Akanksha Saini, Harish Kumar "Comparison between various Black hole Detection techniques in MANET" *NCCI 2010 - National Conference on Computational Instrumentation CSIO Chandigarh, INDIA*, March 2010

[9]. Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M."Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent" *International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012)* July 15-16, 2012 Singapore.

[10]. Monika "Denial of Service Attacks in Wireless Mesh Networks" *(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 3 (3) , 2012.

[11]. A.J. Yuste1, Alicia Trivino, F.D. Trujillo and E. Casilari " Using Fuzzy Logic in Hybrid Multihop Wireless Networks" *International Journal of Wireless & Mobile Networks (IJWMN*), Vol.2, No.3, August 2010.

[12]. Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo" Detecting and Isolating Malicious Node in AODV Routing Algorithm "*International Journal of Computer Applications (0975 – 8887) March 2013*

[13]. V.Gayatri, C .Gomathi "Electing Monitoring node through Fuzzy Theory in Wireless Mesh Network for defense against selective Forwarding Attack" *International Journal of Communications and Engineering Volume 02– No.2, Issue: 02 March2012*

[14]. Timothy J.Ross Mcgraw Hill, Inc, "Fuzzy Logic with Engineering applications"

[15]. A. Baddache, A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *International Journal of Computer Science and Information Security (IJCSIS). USA*, vol. 7, iss. 1, pp. 10-16, January 2010.

[16]. M. Imani, M.E. Rajabi, M. Taheri, M. Naderi, "Vulnerabilities in network layer at WMN," *International Conference on Educational and Networking Technology China*, pp. 487-492, June 2010.

[17]. J. Martin Leo Manickam Anna and S.Shanmugavel ," 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).

[18]. R.A. Raja Mahmood, A.I. Khan "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.

[19]. S. M. Siddiqui, S. C. Hong, "Security issues in wireless mesh networks," *IEEE Inter. Conf. on Multimedia and Ubiquitous Eng. (MUE'07). South Korea*, vol. 1, pp. 717-722, April 2007

[20]. Ben Salem N, Hubaux JP "Securing Wireless Mesh Networks*". IEEE Wireless Communication* (Apr) 2006.

[21]. J. Yin, S. Madria, "A hierarchical secure routing protocol against black hole," *IEEE Int. Conf. on Sensor Net., Ubiquitous, and Trustworthy Computing. Taiwan*, vol. 1, pp. 376-383, June 2006.

[22]. Akyildiz IF, Wang X "A survey on Wireless Mesh Networks". *IEEE Communication Management* (Sept-2005)