JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Eliminating Collaborative Black-hole Attack by Using Fuzzy Logic in Mobile Ad-hoc Network

A. Sharma[1*], P.K. Johari [2]

[1]Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India
[1]Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India

[*]*Corresponding Author: aastha.iitm@gmail.com, Tel.: +91-91799-74877*

Available online at: www.ijcseonline.org

Received: 17/Apr/2017, Revised: 25/Apr/2017, Accepted: 15/May/2017, Published: 30/May/2017

Abstract— Transmitting data securely counter to the mischievous attacks is always concern as a severe issue in an infrastructure less dynamic network called mobile-ad-hoc-network (MANET). Trust assertion between MANET (mobility) nodes is the major attribute for highly secure execution under dynamic topology deflection and open wireless environment. But the mischievous behavior of nodes weakens the trust level of MANET that drags to an untrusted data delivery. The expansion in maligning attacks due to dynamic nature of MANET causes the excessive energy consumption that result in reduction of network lifetime. Trust parameters are adequate to handle the secure route finding procedure. In this composition we also used Fuzzy logic as trusted tool for mitigating the Collaborative Blackhole attack in MANET. This composition recommends a trusted-fuzzy-ad-hoc routing protocol to upgrade the trust between the nodes in MANET. The recommended method customizes the conventional AODV routing protocol. Mischievous behavior nodes are predicted on the basis of mobility based constraints. The packet sequence number is compatible to the log reports of nearby resident nodes, confirms the reliability to the network establishes the trust that avoids the malicious node generation. The result analysis between the proposed technique with the pre-existent technique regarding the routing overhead, throughput, packet delivery ratio shows the effectiveness of trusted-fuzzy-ad-hoc routing protocol in the secure MANET environment.

Keywords—MANET, Routing Protocol, AODV, Collaborative Black-hole Attack, Black-hole Attack

I. Introduction

Wireless networks have considerably evolved in latest years, there is a technology which is extensively are in trend is the mobile_ad-hoc_networks (MANETs). MANET (see Figure 1) relies on infinite no._of_nodes including sender as Originator and receiver as Target inside the network. In different aspect we can illustrate network as “bundle of nodes”. An environment which works globally having infrastructure-less networks without any centralized administration is termed as MANET, composed of number of self-configurable mobile devices, geographically distributed in respected area. Nodes are arranged in dynamic topologies, interfacing by means of multi-hop approach within a communication range. Nodes can publicize directly, while unapproachable nodes make use of other nodes to consign the messages to a given destination. MANET is characterized as dynamic-network-topology therefore it is susceptible to different attacks. Classification of attacks can be sectioned into two parts: 1. External attacks and 2. Internal attacks [1,2,3,4,5,6,7, 8]. The wireless nodes are convenient to both genuine users and attackers. Security solutions become more reliable because of centralized management. An attacker immediately turns into a router and crack network functions [2,4, 9,10]. In MANET each node works as a router. In this composition we suggested a scheme to come across and prevent collaborative Black-hole attack. Our scheme is based on easy Ad-hoc_On_demand_Distance_Vector routing (AODV) protocol.

II. ROUTING PROTOCOL

Routing_protocol is a guide which defines how communication of nodes can be done. This specifies the route between two nodes in network. Routing_protocols have been defined for such form of network. These Protocols discover a route for packet delivery to the correct receiver. The numerous aspects of routing_protocol have been an active region of investigation for several years. Essentially, routing_protocols can be approximately sectioned into three kinds as Proactive Protocols or Table Driven Protocols, On-Demand Protocols or Reactive Protocols and Hybrid Protocols. But, here we are exploring only Proactive and Reactive Protocols.

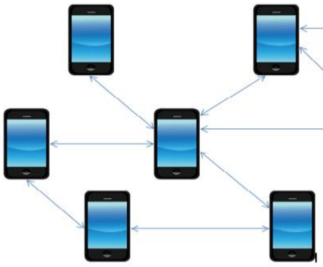

Figure 1. MANET

A. *Table Driven or Proactive Protocols*

In this protocol, nodes can frequently update their routes to every node in the network. Routing notification is regularly communicated all over the network keeping in coordination to maintain routing_table constancy. Existing route will result in depreciated delay in network. Else, packets will wait in queue until the node will acquire the routing notification to its corresponding destination. Though, for high dynamic-network-topology, the proactive patterns necessitate a heavy number of resources to maintain its reliability and routing information. A Proactive routing_protocols we are exploring is DSDV.

1) *Destination Sequence Distance Vector (DSDV)*

In DSDV each node needs to broadcasts its routing_table periodically depends on "BELLMAN-FORD" routing algorithm. The routing_table of every single node comprises certain information i.e, "NEXT_HOP" for all accessible target node, no._of_hop approaches to target and sequence_no. assign through target node. The sequence_no. utilized to prevent loop formation. Each node transmits details of routing_table to their instant neighbors. A routing_table can only share by any node if any changes occurred. So update in both Event Driven and Time Driven approach [3].

B. *On Demand or Reactive Protocols*

In this Protocol, a node starts route detection throughout the network, only when it needs to convey packets to its target. For this purpose, a node starts a route detection procedure through the network. If there is no connection enclosed by the nodes then reactive routing_protocol cannot be maintained. If a node endeavour to convey packet to every corresponding node then the protocol inquires for the route on-demand for and set up the connection for forwarding and obtaining the data package. The reactive routing starts transmitting the data while nodes preference to transmit previous packets.

1) *Ad-Hoc_On_Demand_Distance_Vector (AODV)*

The AODV [4],[5] routing_protocol is an adaptation of the DSDV protocol for dynamic connection conditions. In adhoc network each node hold a routing_table, which contains data and routing information related to route for the target node. Whenever a information bundle is convey by a node, firstly it will review with its routing_table to adjudge whether a path towards target side is existing or not[4]. Basically AODV routing_protocol works on two factors:- 1. RREQ (RoUte_reQuest) and 2. RREP (RoUte_rePly). Because of its request and reply process it is dynamically suggested reliable routing_protocol for transferring the data in MANET. Consider a mobile_ad-hoc_network N (see Figure 2) which is initialized by 8 nodes N1, N2…….N8 among them N1 is originator & N8 target node. Here sender node N1 wants to communicate to destination node N8. So, N1 will send RREQ packet to all their nearby resident nodes i.e, N2 and N3. Every source node required to maintain two counters are: Sequence_No. and Broadcast_ID. Broadcast_ID increments whenever any source node emits fresh RREQ. RREQ packet contains Sequence_No., Source_Seq_No., Broadcast_ID, Destination_address, hop_Count. Now node N2 and N3 broadcast RREQ bundle to their neighboring node and hence all the nearby resident node forwards RREQ packet to corresponding nodes till it reaches to destination node. Finally target end N8 forwards RREP to their corresponding neighboring nodes. The RREP packet contains Source_address, Destination_address, Destination_Seq_No., hop_Count. The node having highest Sequence_No. can be considered for route establishment. As N5 will receive RREP from N8. This same process will follow until all the intermediate nodes forwards RREP to originator side. Therefore, final entertained route will be {N1-N3-N5-N8}.

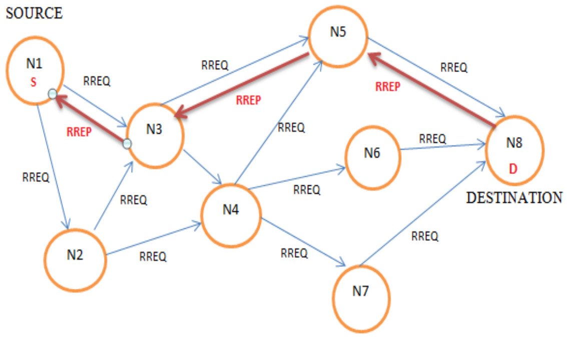

Figure 2. AODV Protocol

Section I contains the introduction of Mobile-ad-hoc-network followed by figure 1 showing network topology of MANET. Section II contains detailed information about routing protocols used over MANET. Routing protocols classifications are explained into 3 categories. Only two routing protocols classification are explained into 3 categories But 2 sub classifications are emphasized most. Section III contains knowledge about Black-hole attack and its functioning. Section IV signifies collaborative blackhole attack and its mischievous activity. Section V provide knowledge on fuzzy_logic and its rules and similarity between fuzzy_logic and MANET. Section VI is about literature survey that had been done by different researchers according to their aspects, parameters and analysis. Section VII is proposed methodology the most interesting section of this composition which will give us detailed information about the proposed work. It is also followed by Figure. 5 flow chart of proposed technique showing step by step working of fuzzy_logic in AODV routing_protocol. Section VIII shows performance evaluation on the basis of packet_delivery_ratio, routing_overhead and throughput with simulation parameters used in experimental simulation. Section IX describes results and discussion on the basis of experiment performed and achieved values provide enhancement over existing technique. Section X concludes the research work with future directions.

III. BLACK-HOLE ATTACK

A black_hole trouble states that single mischievous node employs the routing_protocol to declare itself to be shortest route to the destination, but drops the routing packets instead forwarding data bundles to its nearby resident nodes. A single black_hole attack is effortlessly happened in the mobile_ad-hoc_network. Consider the example (see Figure 3) Node S1 stands for the originator side and node D7 represents target side. Node 2 is a misbehavior node who replies the RREQ bundle received from source node, and makes a fake reply that it has the fastest path to the target node. Therefore node S1 faultily evaluates the route discovery technique, and start sending information bundle to node 2. As mentioned above, a mischievous node quits or consumes the packets. This suspicious node can be seemed as a black hollow problem in MANETs. As a result, node 2 is capable of misroute the packets effortlessly, and the network operation is suffered from this issue[6],[7].

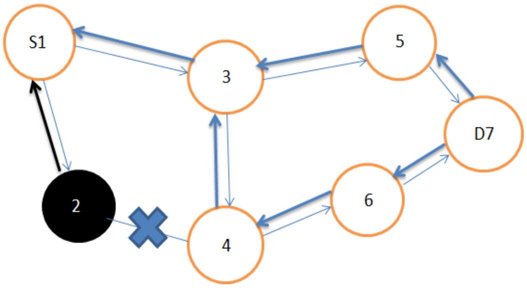

Figure 3. Black-hole Attack

IV. COLLABORATIVE BLACK-HOLE ATTACK

A group of two or more malicious nodes that works in coordination in order to drop and consumes the information bundle that are forwarding between source to destination. Collaborative Black_hole attack is also called cooperative Black-hole or multiple Black-hole attack. These malicious nodes create their own path for dropping the data packets. They pretend that they have shortest path to destination by giving highest sequence no. towards the originator side. In this dilemma source forwards the information bundle to misbehavior node. On receiving information bundles all the information are dropped by the malicious path formed by those misbehavior nodes. Consider the example (see Figure 4) Node 1 is sender node while Node 8 is target side. So, data flow between Node 1 to 8 present in figure. Node M3 and M5 are collaborative Black-hole nodes working in chain scheme. Source node 1 starts forwarding RREQ bundle to corresponding neighbor's i.e, Nodes 2, M3 and 4. As soon as RREQ received by malicious node M3 it will forward RREP packet to originator side 1 that it have simple shortest path towards destination by giving highest sequence_No. Now source node 1 revise their routing_table and start forwarding information bundle to node M3. Once the node M3 start receiving information bundle, it will forwards whole package of information bundle to neighboring malicious node M5 which results in dropping complete information packets. Here node M3 and M5 working in group and hence creating collaborative Black-hole attack.

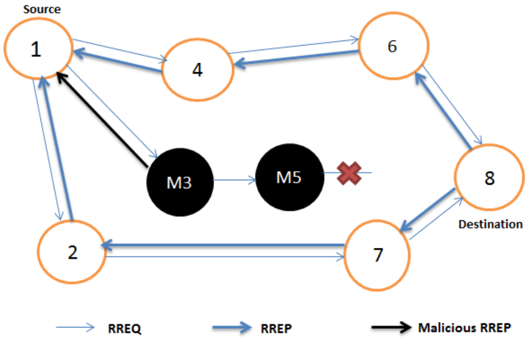

Figure 4. Collaborative Black-hole Attack

V. FUZZY LOGIC

Theory of fuzzy_logic is given by "Lotfi-Zadeh" in 1965[8],[9]. Human observations, actions, behaviour and selection are implemented with the help of membership_functions and fuzzy_rules applying fuzzy_logic. Fuzzy_logic provides a natural framework to deal with uncertainty. There is a similar aspect over fuzzy_logic and MANET deals is "Uncertainty". Uncertainty makes the MANET vulnerable. Basically MANET gives the movability of nodes due to this communication links are vulnerable. Since selecting the safe and abbreviated route for data transmission is very difficult. In communication links there may be part of few malicious nodes for identifying these malicious nodes fuzzy_logic is used to crack the inadequacy. Fuzzy system is very flexible and can change its membership_function and set of fuzzy rules. A membership_function is a mathematical pattern of representing a fuzzy_set.

Assume a set S, a membership_function on S be some function from S to the absolute unit interval [0, 1]. Membership functions on S represent fuzzy subset of S. The membership_function set is generally denoted by µX. For an element s of S, the value µX(s) is labeled as membership_degree of s in the fuzzy_set. • µX(s) =0 implies s is not a member of fuzzy_set S.

• µX(s) =1 implies s is fully member of fuzzy_set S.

• µX(s) among 0 and 1 represent fuzzy members, which belongs to set S partially.

VI. RELATED WORK

In [10] recommended a scheme to keep away from such an coordinated attack called black_hole attack by means of calculating agree with cost at each node the usage of only control packets which enables in reducing routing overhead. Ad hoc wirelessly networks are defined due the class of wirelessly networks which exploit multi-hop radio relaying and are accomplished of running with no the support of any constant infrastructure and as a outcome they're additionally called infrastructure much less networks. This kind of network permits for spontaneous communication without previous planning between cellular gadgets. A type of routing protocols for ad hoc wirelessly networks has been define in current past but AODV protocol is famous due to its dynamic nature that is routing statistics is exchanged and direction locating manner is initiated handiest when path is needed by means of a node to talk with a destination node. Attack is launched on this protocol if an middle node maliciously behaves during the direction locating procedure and drop packets which goes through it. This attack becomes more severe if group of nodes co-coordinately work to launch this attack.

In [11] presents an Individual Trust Managing Method to prevent against sink-hole attack. In this research sinkhole attack is implemented for analyzing different effects on n/w performance due to increasing the mobility and probability of attacks. A detection approach is also analyzed for effective elimination and detection of attacker node. The suggested analysis is simulated utilizing network simulator NS3. In this way, the ad-hoc networks are exploited by RP design. So, there is need of methods to make MANET routing protocols resistant to Sinkhole attack. In this research work, the Sinkhole attack has been executed over AODV. The prevention technique is significantly successful in handling the attack while restoring the n/w performance and reduces the effect of attack from the network [11].

In [12] this composition, they define a hybridization of the Firefly and the ACO, swarming algorithm (FA) for AODV RP to rise the efficiency in the transmission of the signals in a MANET system and thus intending to considerably decrease the losses, so incurred using solely the AODV and overcome weaknesses of ACO depend AODV. They create comparative analysis on the define hybrid algorithm with the present routing algorithms ACO depend AODV thereby make sure decrease of n/w load by avoiding re-detection attempts amid the nodal [12].

In [13] defined an enormous method which depends on adaptive FIS-fuzzy_inference_system for MANET in sequence to detect and prevent the co-operative black_hole attack. The popular protocol utilized in MANET is AODV protocol, and is simulated exploiting NS2. The simulated results of the define method are compared with that of an adaptive method, wherein source node checks all nodes activity by using DAT table that maintains from-node-to-next node's info and declares black_hole node through channel overhearing technique. It's observed that the define approach depend on adaptive fuzzy_logic system demonstrations better performance as equated to adaptive technique in terms of end-to-end delay, PDR, and throughput.

In [14] did a tremendous research, by checking DOS attacks called as black_hole attack. In this attack, a mischievous node broadcasts an incorrect route through itself as the mostly valid path and compact to the target. Using this fabricated route the malignant node schemes to intercept and dump all records packets supposed for the target side node. A method employing SAODV (secure AODV) routing algorithm is recognized. Revealing and intercepting black_hole attacks in mobility network is done in this composition. Here they exploit watchdog scheme as an upload-on in SAODV routing algorithm for prevention and discover of the black hole_nodes in the MANET. The define methodology enhances the PDR and performance in the occurrence of numerous black_hole_nodes in MANET.

In [15 the composition, define the black hole-worm hole avoidance and detection algorithm of FPGA. The packets from a black-hole or worm-hole are identified inside the MAC-Physical layer itself through exploiting randomly varying the Packet Travel Time (PTT). The physical layer and Mac layer are implemented the usage of Partial-Reconfiguration method so that the symbol rate, modulation patterns and coding charge may be changed randomly while the system is running without exploiting additional hardware. Authentication is used to ensure the RREQ_request and RREP_response messages in network.

In [16] is Fuzzy IDS, This proposed framework gives the honorable arrangement and distinguish the attack is clearer by utilizing the fuzzy_logic procedure. The framework additionally contains IPS system procedure which gets contribution from fuzzy strategy and gives the protected data correspondence over the network. IPS additionally screen for the movement of black hole and gray hole attacks. The outcome unmistakably demonstrated this technique recognizes the assault in an effective way when contrasted with existing technique. Future work incorporates the lessening of jitter value which is more in nearness of IPS, which is a direct result of course adjustment in nearness of attacks.

VII. PROPOSED METHODOLOGY

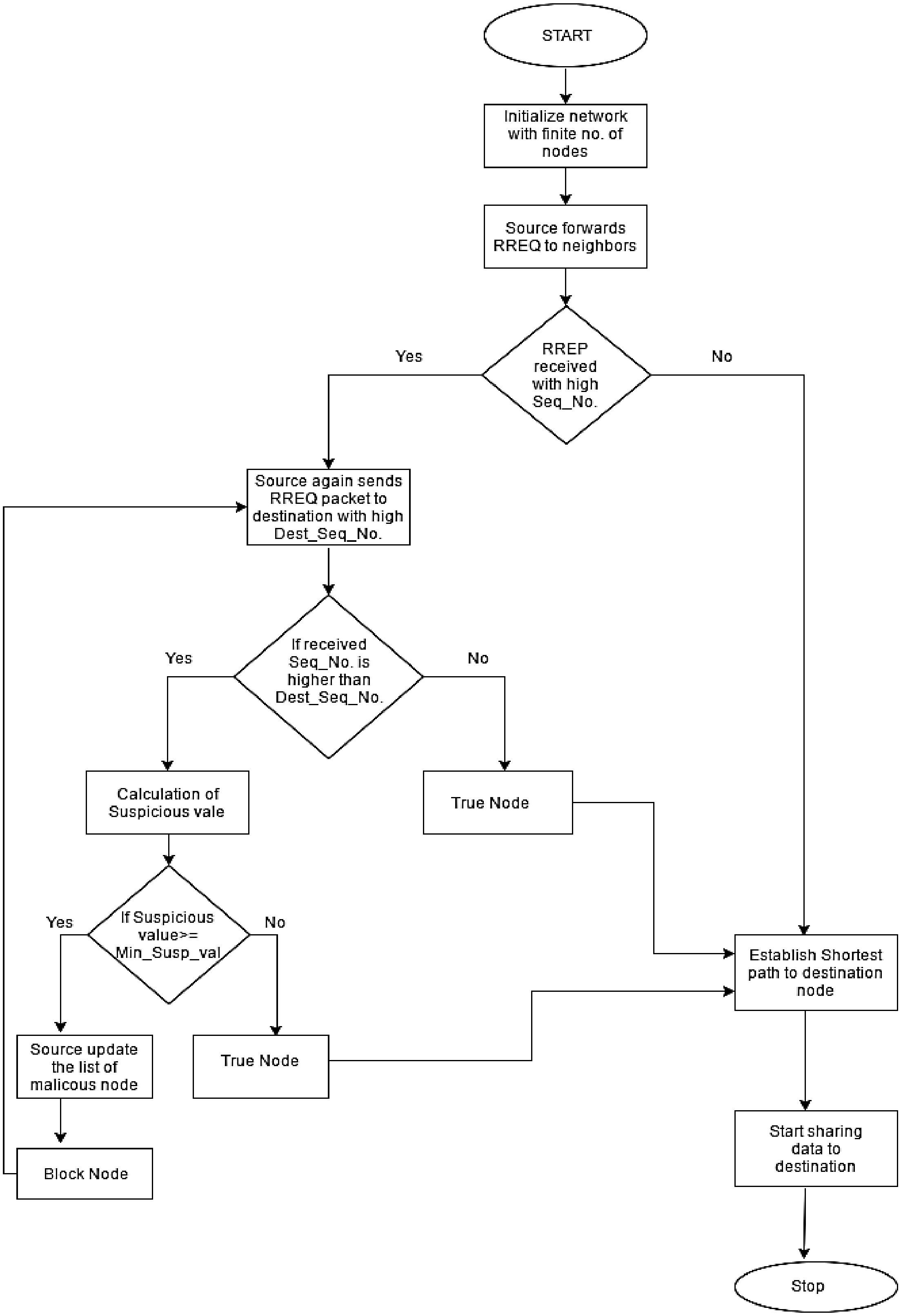
START
Initialize network with finite no. of nodes
Source forwards RREQ to neighbors
RREP received with high Seq_No.
Yes
No
Source again sends RREQ packet to destination with high Dest_Seq_No.
If received Seq_No. is higher than Dest_Seq_No.
Yes
No
Calculation of Suspicious vale
True Node
If Suspicious value>= Min_Susp_val
Yes
No
Source update the list of malicous node
True Node
Block Node
Establish Shortest path to destination node
Start sharing data to destination
Stop

Figure 5. Flow Chart for suggested Methodology

Due to internal and external attacks in MANET, performance of network is compromised. MANET is surrounded by several attacks but emphasizing domain is Collaborative Black-hole attack. It is considered as strongest attack and works in group since it will discard complete information packages (see Figure 4) once connection will established between the originator and the malicious node. According to their nature collaborative Black-hole attack acts as legitimate node and start dropping the packets. For identifying this problem we have suggested fuzzy_logic in routing_protocol AODV. This technique will help us in identifying multiple malicious nodes. Resulting because of network congestion or buffer overflow several nodes drops some packets, these nodes are not malicious but it behaves maliciously. So to discriminate between misbehavior nodes and malicious nodes we have suggested our new technique. Let us consider two conditions:

- Node is Suspicious but not Malicious.
- Node is Suspicious but also Malicious.

We are giving an algorithm for recognising and restricting the collaborative black-hole attack. Without any modification in network the sender can efficiently identify and prevent the collaborative black-hole attack. Suggested technique subsists in 2 procedures:

- Collaborative Black-hole nodes identification during the path discovery phase of the AODV routing_protocol.
- Removal of collaborative black-hole nodes from the network.

Both the raised steps can be followed by using fuzzy_logic. This will ensure us genuine nodes will never treated as malicious node and also improves the performance and efficiency of network. Figure 5 will explains the functioning of entire process.

VIII. PERFORMANCE EVALUATION

We are evaluating performance of network in terms of Packet_Delivery_Ratio, Routing_Overhead and Throughput.

- Packet_Delivery_Ratio: P_D_R is a ratio of total no._of_packets received at destination to total no._of_packets sent by source.
- Routing_Overhead: R_O is total no._of_routing_packets divided by total no._of_delivered_data_packets.
- Throughput: T_P is the no._of_packets successfully received per second.

Table 1. Simulation Parameters

Constraints	Description
Simulator	NS-2
Total nodes in Simulation	10,20,30,40,50,60,70, 80,90,100
Simulation Time Period	120 second
Type of traffic	Constant bit rate (UDP)
Simulation Area	500*500 sq mtr
Packet Size	512 Byte
Routing Protocol	AODV
Network interface type	WirelessPhy
Internet Protocol	IPV4
MAC type	802.11
Antenna Model	Omni antenna
Maximum Speed	20 m/s
Channel type	Wireless channel

IX. RESULTS AND DISCUSSION

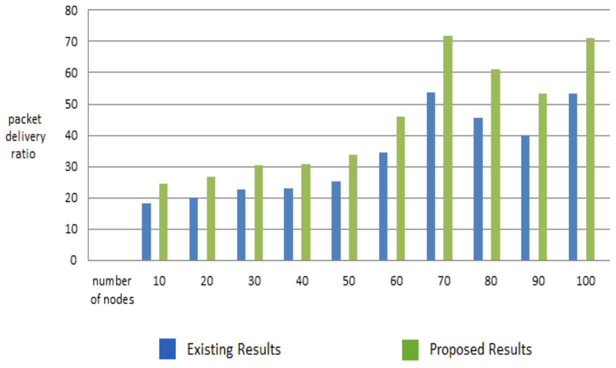

Figure 6. Packet_Delivery_Ratio Simulation

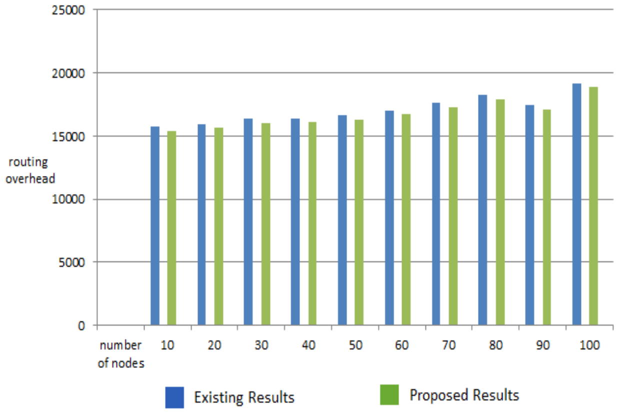

Figure 7. Routing Overhead Simulation

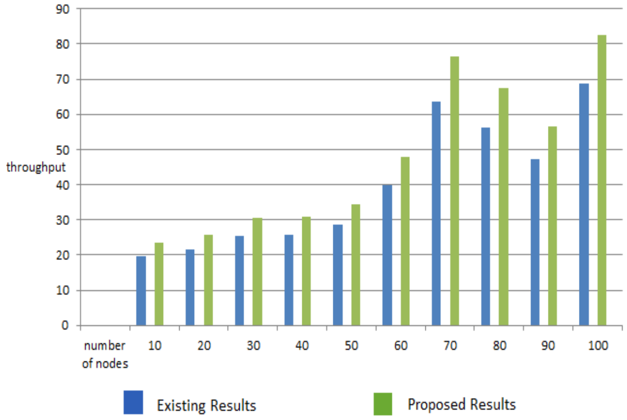

Figure 8. Throughput Simulation

Table 2. Comparison of fuzzy implementation over existing technique in terms of Packet_Delivery_Ratio

No. of nodes	**Packet Delivery Ratio**	
	Existing_AODV	***Fuzzy_AODV***
10	18.39	24.53
20	19.95	26.60
30	22.83	30.44
40	23.19	30.92
50	25.35	33.80
60	34.54	46.05
70	53.72	71.63
80	45.76	61.01
90	39.89	53.19
100	53.32	71.10

Table 3. Simulation Parameters Comparison of fuzzy implementation over existing technique in terms of Routing Overhead

No. of nodes	**Routing Overhead**	
	Existing_AODV	***Fuzzy_AODV***
10	15730	15428
20	15900	15638
30	16385	16009
40	16403	16096
50	16646	16315
60	17045	16724
70	17638	17306
80	18230	17911
90	17449	17130
100	19169	18847

Table 4. Comparison of fuzzy implementation over existing technique in terms of Routing Overhead

No. of nodes	**Throughput**	
	Existing_AODV	***Fuzzy_AODV***
10	19.6833	23.62
20	21.57	25.884
30	25.61	30.732
40	25.8167	30.98
50	28.8017	34.562
60	39.84	47.808
70	63.6083	76.33
80	56.2283	67.474
90	47.2483	56.698
100	68.7617	82.514

Figure 6, 7 & 8 states enhanced simulation outcomes, hence it strengthen the network's efficiency. Green colored simulation showing enhanced outcomes over red colored simulation. Table 1 specifying the simulation specification we have adopted in our composition. Table no. 2, 3 & 4 exhibiting upgraded conclusions over previous researches.

X. Conclusion and Future Scope

This composition discusses how the fuzzy_Logic is implemented over routing_protocols in the Mobile ad-hoc network. The respective implementation helps us in finding most favorable and reliable route towards destination for sending data packets. In this possibility of blocking true nodes are reduced. Multiple malicious nodes can harm the network hence it was highly challenging identify the node dropping the data packets. In simulation we have used 10,20,30,40,50,60,70,80,90,100 nodes on the basis of Packet_Delivery_Ratio, Throughput and Routing_Overhead. The proposed composition is based on fuzzy technique therefore overall performance is analyzed and resulted Packet_Delivery_Ratio is 33.33% improved, Throughput is 20% improved and Routing_Overhead is 1.87% reduced over existing_AODV. Since, it becomes very impactful in determining and terminating those Collaborative Black-hole nodes. Hence this methodology will provide us maximum quality_of_service and improvement in network performance. In future this approach is extended to enhance the performance of MANET under Grayhole Attack and Wormhole Attack.

Acknowledgment

The authors would like to thank the anonymous reviewers for their constructive comments.

References

[1] S. Banerjee, R. Nandi, R. Dey, H.N. Saha, "*A review on different Intrusion Detection Systems for MANET and its Vulnerabilities*", In the Proceedings of the 2015 IEEE International Conference and Workshop on Computing and Communication (IEMCON), Canada, pp.1-7, 2015.

[2] N.K. Pandey, A.K. Mishra, "*An Augmentation in a Readymade Simulators Used for MANET Routing Protocols: Comparison and Analysis*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.60-63, 2014.

[3] Mewada Shivlal, Sharma Pradeep, Gautam S.S., Sharma Sarita, Agiwal Priyanka, Shrivastava Arti , "*Simulation Based Performance Analysis of DSDV OLSR and DSR Routing Algorithm in Wireless Personal Area Network Using NS-2*", Research Journal of Computer and Information Technology Sciences, Vol.4, Issue.1, pp.1-7, Jan 2016

[4] N. Mannan, S. Khurana, "*Comparative Analysis of Reactive Protocols in Mobile Ad-Hoc Networks*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.4, pp.233-237, 2014.

[5] I.D. Chakeres, E.M. Belding-Royer, "*AODV Routing Protocol Implementation Design*", In the Proceedings of the 2004 IEEE 24th International Conference on Distributed Computing Systems Workshops, Japan, pp. 698-703, 2004.

[6] F.H. Tseng, L.D. Chou, H.C. Chao, "*A survey of black hole attacks in wireless Mobile ad-hoc networks*", Human-centric Computing and Information Sciences, Vol.1, Issue.1, pp.1-4, 2011.

[7] UK Singh, J Patidar, KC. Phuleriya, "*On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.1, pp.11-15, 2015.

[8] S.V.S.G. Devi, "*Prediction Of A Class Variable In Classification Problem Using Fuzzy Inference Method*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.1, pp.28-29, 2014.

[9] L.A. Zadeh, "*The Role of Fuzzy Logic in the Management of Uncertainty in Expert Systems*", Fuzzy Sets and Systems, Vol.11, Issue.3, pp.199-227, 1983.

[10] J. Thakker, J. Desai, L. Ragha, "*Avoidance of Co-operative black hole attack in AODV in MANET*", In the Proceedings of the 2016

IEEE International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, pp.1-7, 2016.

[11] Vaishnavi Katkar , Sagar Indore, Tushar Pokharkar, Kajal Inamdar, "*Detecting Spam Zombies by Monitoring Outgoing Messages and DoS View*", International Journal of Scientific Research in Network Security and Communication, Vol.4, Issue.1, pp.5-11, 2016.

[12] S. Nath, S. Banik, A. Seal, S.K. Sarkar, "*Optimizing MANET routing in AODV : An Hybridization approach of ACO and Firefly Algorithm*", In the Proceedings of the 2016 IEEE Second International Conference on Research in Computational Intelligence and Communication Networks, Kolkata India, pp.23-28, 2016.

[13] P.S. Hiremath, T. Anuradha, P. Pattan, "*Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs*", In the Proceedings of the 2016 IEEE International Conference on Information Science, Kochi India, pp.145-151, 2016.

[14] B. Chandra, N.P. Shetty, "*Interception of Black- Hole Attacks in Mobile AD-HOC Networks*", In the Proceedings of the 2016 IEEE International Conference on Inventive Computation Technologies, Coimbatore, India, pp.105, 2016.

[15] PK. Sharma, SL. Mewada, P. Nigam, "*Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.4, pp.8-11, 2013.

[16] E.V. Balan, M.K. Priyan, C. Gokulnath, G.U. Devi, "*Fuzzy Based Intrusion Detection Systems in MANET*", 2nd International Symposium on Big Data and Cloud Computing, India, pp.109-114, 2015.

[17] V. Thakur, L. Shrivastava, S.S. Bhadauria, "*Performance Evaluation of AODV Using Fuzzy Logic to Reduce Congestion in MANET*", Asia-pacific Journal of Multimedia Services Convergent with Art Humanities and Sociology, Vol.5, Issue.5, pp.1-9, 2015.

[18] A, Chaudhary , A, Kumar , V.N. Tiwari, "*A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs*", In the Proceedings of the 2014 IEEE International Conference on Reliability, Optimization and Information Technology, Faridabad India, pp.178-181, 2014.

[19] S. Madhurikkha, C.M. Kumari, S. Revathi, P. Nathiya, "*Preventing Packet Dropping Attack in Ad hoc Networks Using Malicious node Isolation Model*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.3, pp.72-177, 2015.

[20] K. Narang, "*Black Hole Attack Detection using Fuzzy Logic*", International Journal of Science and Research (IJSR), Vol.2, Issue.8, pp.222-225, 2013.

[21] Bhagyashree Thakur, Sharda Patel, Ashok Verma and Shivendu Dubey, "*Simulation Of Blackhole Nodes And Prevention Using IDS For MANET Reactive Routing Protocol AODV*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.12, pp.114-120, 2014.

Authors Profile

Miss Aastha Sharma pursed Bachelor of Engineering in Information Technology from RGPV, Bhopal in 2013. She is currently pursuing Master of Technology in Cyber Security from RGPV, Gwalior. She is a member of IET since 2016. Her main research work focuses on Network Security.

Mr P K Johari pursed Master of Technology in Information Technology form RGPV, Bhopal in year 2006. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science and Engineering and Information Technology, MITS, Gwalior since 2010. He is a member of IET & CSI since 2016 & 2015, a life member of the GAMS since 2006 and IAENG since 2012. He has published more than 20 research papers in reputed international journals including Thomson Reuters and conferences including IEEE and it's also available online. His main research work focuses on Computer Vision, Data Mining and Network Security. He has 12 years of teaching experience and 5 years of Research Experience.