I. J. Computer Network and Information Security, **2017, 7, 29-35**
Published Online July 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.07.04

Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology

Ashish Kumar Khare
PhD Scholar, SATI, Barkatullah University Bhopal, India
E-mail: prof.khare@gmail.com, prof_ashish@rediffmail.com

Dr. J. L. Rana and Dr. R. C. Jain
Ex-HOD, CSE, MANIT, Bhopal, India
Ex-Director SATI, Barkatullah University Bhopal, India
E-mail: jl_rana@yahoo.com,dr.jain.rc@gmail.com

Abstract—Mobile ad-hoc communication is a spontaneous network because the topology is not stationary but self-organized. This requires that during the time MANET it operational, all the processes regarding discovering the topology, delivery of data packets and internal management communications must be taken care by the node(s) themselves. This implies the criteria for selection of Cluster Head (CH) and the routing related protocols are to be integrated into mobile node(s).The very facts that MANET is challenging and innovative areas of wireless networks, makes it more vulnerable in term of routing and flooding attacks. In this paper, a node trust calculation methodology is proposed which calculate the trust value of each node and applies fuzzy logic to detect wormhole, Black-hole (Routing attack) and distributed denial of service attack (DDOS/Flooding) in dynamic environment.

Index Terms—MANET Security, Attack Detection, Trust Calculation, Fuzzy Logic.

I. Introduction

A MANET is a high capable and fast moving technology. It is a key step in the evolution of wireless networks. The evolution of wireless networks plays vital roles in present day society. Limitations of infrastructure need for self-organization and dynamic change of node(s) are the main characteristic of Mobile Ad Hoc Networks. The communication occurring in wireless mode (open method) makes the MANETs more susceptible to security attacks. By the use of various security protocols, effect of various attacks can be reduced. The mobile hosts dynamically discover route(s) amongst themselves so that messages in the form of data packets can be sent from one node to the other node. Success of data communication depends on the mutual co-operation of the complex mobile node(s). The major problem with MANET is its vulnerability to security attacks [1]. The security challenge has become a major concern. The problem is further aggravated by mobility of nodes in random manner, nodes coming and leaving the in unpredictable way. Resource constraints specially affect the energy, bandwidth and memory computations needs while route table updating. All these things make providing trust in MANET an additional critical task more so because of lack of centralized infrastructure. Although MANETs are not difficult to execute, the implementation becomes problematic because they're more venerable to threats and attacks, primarily because distributed nature of services create several weak points in security [2,3]. In this paper all the important reported techniques have been systematically categorized and their strong and weak points have been discussed. Based on these and the current technical scenario suggestions have been proposed for upcoming research guidelines on attack detection and trust management schemes. Various others challenges based on trust measurements and attacks in MANETs have also been discussed.

II. Related Works

In most of the reported literature, trust level of node(s) has been made the focal point. The difference is in the ways in which trust level is calculated and quantified and later its application in securing the network communication. A trust based approach to improve security between Node(s) using fuzzy logic has been proposed by H.Hallani et.al [4].With the objective of mitigating the cause of malicious node(s) and to achieve higher levels of security and consistency, authors have developed a novel scheme which incorporates appropriate fuzzy logic concepts in their proposed algorithm to set up quantifiable trust levels amongst the node(s) of MANET. The quantified trust levels are then used in making routing decisions. This facilitates in deciding the most secure route during the routing discovery. Along with fuzzy logic, Suresh Kumar et.al [5] have proposed a Node Transition Probability (NTP) routing algorithm which uses a control packets to determine the routes

between for sources and destination nodes. The proposed algorithm adapts rapidly to routing changes when node(s) movement is frequent. NTP along with the fuzzy logic for routing, appear to be promising, however implementation in MANET is resource intensive. As such NTP is not ideal with regard to trade-offs between efficiency and effectiveness.

There are some other alternatives that work nicely in the presence of one compromised node, but the effectiveness is lost when multiple attackers that are colluding. For discovering the malicious node(s) a novel method has been proposed by Sakshi Jain and Ajay Khuteta [6]. Their method is based on Base Node (BN) sending dummy RREQ packet at every time interval. Normal nodes do not send reply as the dummy RREQ is for node that do not exist in network. Only malicious nodes will send a reply since they do not check in their table for route to destination and start generating route reply message. BN node thus detects that malicious node and shares it with all the normal nodes for blocking the communication to and from these malicious nodes. This technique greatly reduces the possibility of black hole attack in network and also reduces energy and delay in MANETs. Using similar concept Farrukh Aslam Khan et.al[7] have designed a detection and prevention system (DPS) against collaborative attack in MANETs. In their proposed method, all transmitted RREQs packet are regularly monitoring by additional node(s) (DPS Nodes) in the network. After analysis DPS Node(s) identify suspicious node(s) and broadcast block message for these malicious nodes to the network.

A different approach is used by Dhiraj Nitnaware and Anita Thakur [8]. Authors have designed DYMO-AODV protocol based on BDS mechanism; that modifies the AODV protocol. In this approach there are three steps:- Broadcast Hello packet, Suspicious Node Detection and Suspicious Node Prevention. Each and every node receives broadcasted hello packet and processes the capability check of every mobile node. Here, Hello packet hides the detection mechanism which collects the hardware information of current node and verifies this with threshold value. If any node is observed with extra ordinary capability it is considered as the malicious node and this information is forwarded to prevention mechanism.

Using somewhat similar technique Nitika Gupta and Shailendra Narayan singh [9] proposed a digital signature technique to prevent the wormhole attack in networks. Cluster head (CH) and Cluster gateway (CG) maintain the communication between the nodes or two clusters by using public keys authentication technique. The proposed protocol is preventing the wormhole attack with cryptography concept but without using any complex hardware implementation.

H.Vignesh Ramamoorthy and Dr.D.Suganya Devi[10] have proposed a cohesive approach using a small number of control packet to recognize a relatively optimum path for routing.A substitute route is pre computed for any route failure during data transfer. The recommended scheme is multi agent ant-based routing which has combined the feature of proactive and reactive concept in one routing protocol. The proposed hybrid routing protocol provide better performance in scalability feature and connectivity of nodes. The offered integrated approach has also a minimized the end-to-end delay and the route discovery latency

Partha Sarathi Banerjee et.al.[11] have proposed trust based AODV routing protocol that works with three fuzzy logic based membership functions- PI-membership function, Gaussian membership function and Triangular-membership function for trust value calculation using multi criteria to identify untrusted neighbors. Only trusted neighbors are used for packet transfers. Authors have presented an approach that yields better throughput in absence of selfish node. Key focus of the scheme is to send packets over a wireless medium with energy efficient and negated of malicious node.

Tarunpreet Bhatia and A.K. Verma [12] have highlighted the Black hole attack effect on AODV routing in MANRT and gave a solution for overcoming the malicious influence. Authors analyze the different scenarios under various parameters to evaluate the damages caused to the network. they gave an efficient security functions to apply ton AODV protocol as solution to overcome black hole attacks. The simulation reports show that occurrence of blackhole nodes will cause an adverse effect on the AODV performance like packet delivery fraction, number of dropped packets, throughput and normalized routing load.

Using Cryptographic Algorithm Disturbance Detection System (DDS) for MANET has been proposed by M.Madhurya et. al.[13]. In this method authors have developed a shared decision making system based on any data exchange in the network by multiple threshold values .The protocol is design for condition based routing which provides fast response to self-motivated connection requiring less memory overhead and low processing . Cryptographic algorithm encrypts the data packets for ensuring the security through authentication.

Soumyabrata Talapatra and Alak Roy [14] define a concept clustering for MANET that facilitates the researcher use of effective and efficient clustering schemes for MANETs. The proposed algorithm provides a better solution for cluster maintenance by minimum message passing scheme and saves resources. Scheme is suitable for limited scenarios, there is no guaranteed for suited to all situations.

Routing protocols (AODV-Ad-hoc On Demand Distance Vector Routing, OLSR-Optimized Link State Routing, DSRD- Dynamic Source Routing and DSDV-Distance Sequenced Distance Vector) have been studied by Rakesh Kumar Jhaand and PoojaKharga[15]. They have simulated these four protocols with different set of parameters and under different situations to check the effectiveness of particular protocol. The outcome of simulation shows that AODV is definitely superior to the other routing protocols in the context of throughput for network having frequently changing number of nodes. OLSR protocol gives good result interns of the end to end delay, jitter, packet delivery ratio and Packet dropped.

NitinKhanna[16] has enhanced AODV routing protocol by adding Cryptography and Trueness Level for efficient response to different types of packet drop attacks. This is achieved by mitigating them through avoidance and elimination of source of attack after detection. The proposed design system effectively uses cryptography and provides secure environment with minimum Cryptography overhead. It is highly suitable for popular packet drop attacks Gray hole attack, Blackhole attacks and cooperative Blackhole attack etc.

III. The Proposed Work

Security is a critical challenge for unstructured network nodes participating in communication in MANET. While using the TCP prototype module for the communication every layer level security is must if highly reliability is needed during the communication. But in data transmission phase under mobile ad-hoc communication, routing layer and data link layer security is mandatory. Because number of different types of attackers, attack the network layer eg. black hole, wormhole, gray hole, Sybil etc. similarly in data link layer denial of service (DoS), DDoS, flooding etc. are the identified attackers which easily capture the genuine nodes and access the important data or mislead. In mobile ad-hoc network, it is critical to detect these above mentioned attacks. In our proposed work real time detection of the wormhole, black-hole and DDoS attack is done with node trust estimation using fuzzy logic methodology. This is applied to the Ad-hoc on demand distance vector (AODV) routing to establish the shortest path. We initially assign the trust value of each node as zero by default. After that sender sends the data through established path and we calculate the updated trust value while intermediate node(s) receive the incoming packets from predecessor node and forward or not forward .The received packet. Based on data forwarding trust value are calculated through every nodes in every receiving and forwarding events.

Initially we define trust value of each node as zero. In the process of receiving and forwarding the data the trust value of each is increased or decreased by 0.05 based on data forwarding criteria. The latest session of forwarding and receiving ratio is compared with old ratio. If that value is equal or greater than the previously stored value than the trust value of the particular node is increased by 0.05 else decreased. The trust value of the node varies in the range in between -1 to 1. Here, -1 means un-trusted node and 1 means highly trusted node. Trust value can be useful to identifying potential attacker nodes within the network. There are seven levels of trust values. As shown in table 1 below and helps to detection of attacker node. These crisp values are later used in fuzzy logic based trust assignment methodology.

Table 1. Fuzzy Based Trust Assignment

Criteria	Category	Crisp Value
I_{t1}	un-trust	-1
I_{t2}	initial-trust	0
I_{t3}	very-low-trust	0.2
I_{t4}	low-trust	0.4
I_{t5}	moderate-trust	0.6
I_{t6}	trust	0.8
I_{t7}	high-trust	1

A). Algorithm: Detection Wormhole/Blackhole/DDOS

Informal Description of Algorithm:

This section two algorithms are described. First algorithm uses details with respect to input, output needed for identifying the effects of attacks and its symptoms. The second algorithm, describes the procedure to calculate trust value for each node and generation of crisp value that characterizes level of trust of every node useful in identifying the attackers.

Algorithm-1:

The algorithm-1 accepts the input as ID and number of mobile nodes and their related parameters. Using these and the values coming from altorithm-2, it manages and sets the sender/receiver nodes and all aspect of mobile ad-hoc communication parameter that help to retrieve the output in the form of attacker node identification, percentage of attacks etc. During the algorithm execution, number of different attack cases is defined. If the attack case is a black hole attack then the algorithm-1 makes the sender initiate the route broadcast routine, that packet contain the sender id, receiver id, intermediate id (if broadcasted packets is received by Intermediate nodes) and radio range. While intermediate node (I-node) is within the radio range but it is not a designated receiver, than I-node(s) (if suspicious designated as I_s) generates the higher sequence number and sends back this sequence number as a reply to sender. Those packets so received spoof the sender and sender initiates sending the data over wrong routes. Similarly in DDoS attack case if an I-node is attacker, this attacker node floods the unwanted message to all the respective neighboring nodes and captures (drowns) them. Thus flooding is spread in distributive manner and engulfing the entire network. Lastly, a wormhole attack is a network layer attack, where two or more nodes participate in this type of attack. In a typical wormhole attack node1 (say) receives data from predecessor and forwards this to next wormhole partner (say) node2. Such data/messages are then partially captured or dropped and partially forwarded to genuine receiver making this type of attack critical and difficult to detect. In the proposed algorithm detection of the attacker node through symptoms matching based approach is described. It provides the necessary basis for future attack prevention methodology.

Formal Description:

Input:

M: set ofl number of k nodes
m_i: A single Node; i=1,2,3…..k
S: Sender nodes ϵ M
R: Receiver nodes ϵ M
I: Intermediate nodes ϵ M
Sp: Suspicious nodes
I_s: Intermediate Suspicious nodes
I_i, I_{i+1} Wormhole tunnel nodes pair
Loop: Message suspicious nodes not forwarding data (In blackhole) Wormhole
C: Symptoms
Ψ: Radio Range in Meters
U: un-trusted message
Idle: Not participating in routing
Output: Attacker identification, percentage of attack, type of attack, PDR, Routing load

Case1: Blackhole

S_Route_Bcast(S, I, R, Ψ)
While I_i in Ψ && I_i != R do
I_s←Generate-higher Seq No. //OnlyBlackhole(s) generate the seq No.
I_s →RREP to S
Send(S, I, data)
End do

Case2: Wormhole

While I_i in Ψ && I_i != R do
I_i →forward routing packets to I_{i+1}
I_{i+1}← receive routing from I_i
I_{i+1_RREP}← I_{i+1} send route reply to S via I_i
Send(S, I_i, data)
End do

Case3: DDoS

I generate U
Bcast(I, m_i, U)
If m_i is idle && m_i in Ψ Then
m_i ← receives U

$$\text{I send U to } m_i = \sum_{i=1}^{k} M_k \quad (1)$$

m_i is busy and not responds to genuine senders
Goto Case3 while m_i != (M_{k-1})
End if

Default:

Normal routing of AODV(S, R, Ψ)
Send(S, R, data)
End case
Send(S, I, data)
If C != Normal-profile then
Set I as S_p
If S_p == Loop then
I ← drop/capture data
C← blackhole
elseIf S_p == forward then
I_{i+1}←receives from I_i
I_{i+1}←Selective drop and capture data
C← wormhole
End if
End if
Stop

B). Trust calculation with Fuzzy set

Algorithm 2:

In this section calculation of node trust level with the help of crispy sets is described. Initially fuzzy set value, trust variance etc are defined. In the initial case all node trust level values are set as zero and later updated based on test ratio of the number of data packets forwarded out of data packets received by the node. If the new ratio is greater than the previous one then trust level value is increased by 0.05. Otherwise it is decreased by 0.05. At the end all these values are entered in a trust table and the level of final trust value of each node is assigned crisp value. Entries of this table are analyzed to identify the attacker nodes.

Algorithm2: Trust Estimation of Nodes

Initialization:

F: Set of Fuzzy values {-1, 0, 0.2, 0.4, 0.6, 0.8, 1}
∂: Trust-update (+/-) 0.05
T: Trust-value (0.0)
I_P: initial performance (0.0)
Output: Fuzzy based Trust calculation P: performance
Procedure:
T_{old} = T
If I receive (data, S) then
P = Packet forwarded/ Packet received
If (P >= I_p) **then**
T_{new}← T_{old} + ∂
I_p← P
Else If (P < I_p) **then**
T_{new}← T_{old} - ∂
I_p← P
End if
End if

T in F set

Generate trust table

I_{t1}← un-trust (F = -1)
I_{t2}← initial-trust (F = 0)
I_{t3}← very-low-trust (F = 0.2)
I_{t4}← low-trust (F = 0.4)
I_{t5}← moderate-trust (F = 0.6)
I_{t6}← trust (F = 0.8)

$I_{T7} \leftarrow$ HIGH-TRUST (F = 1)
Stop

IV. Simulation and Experiment

A. Simulation Results

ns2-2.34 is used to evaluate the performance of the network using AODV Protocol, first without attack and later under different types of attack. In simulation we have used 50 mobile nodes with base routing protocol as ad-hoc on demand distance vector (AODV) routing and have considered three similar environments for analysis about the behaviour of AODV namely without attack, under wormhole attack and blackhole as well as Distributed denial of service (DDOS) attack. Different matrices like Data packet sent, Data packet received, Data packet drop, Routing load and Packet Delivery Ratio have been used to evaluate the performance of network. The simulation parameters are shown in table 2.

Table 2. Simulation Parameters

Parameters	**Type**
Physical Medium	Wireless Phy
Propagation Modes	TwoRayGround
Antenna Type	Omni Directional Antenna
Simulation Area	800*800 m^2
Simulation Time	100 seconds
Frequency	914e+6 Mhz
Routing Protocol	AODV
Attack Type	Wormhole, Blackhole, DDOS
Detection Methodology	Trust Estimation of nodes, Fuzzy rules
Traffic Type	CBR
Agent Type	TCP/UDP
Node Mobility	Random(0-20 m/s)
No of node	50
Radio Range	550m
Packet Size	1024Kb

Firstly the trust estimation based detection is applied for calculating trust level of nodes using fuzzy logic. Thereafter we analyze the performance of the network under three types of attacks within the network and also to capture, drop or unwanted packet spread over the network. This process identifies all the attacker nodes which have un trusted value (-1). The table 3 below shows the identified denial of service attacker nodes 5,12,25,27 and 32 whose unwanted packets flooded nearly 96% in the network in collaborative attack-(second attackers being black hole attack nodes 25 and 32 which cause 5% data drop. The proposed detection methodology detects simultaneous blackhole-ddos attack (blackhole in collaboration with ddos). Cumulatively this attack decreases the network performance by 96.5%. Under wormhole attack scenario node 32 is detected as an attacker node that drops nearly 25.23% of data from the network.

Table 3. Attacker Node Analysis

Attacker Node Analysis		
DDOS Attacker	**Packet Spread**	**Percentage of Spread**
5	5642	2.11
12	37854	14.16
25	142137	53.17
27	150	0.06
32	70644	26.42
Black hole Attacker	**Packet Drop**	**Percentage of Drop**
25	1094	0.41
32	110	0.04
Wormhole Attacker	**Packet Drop**	**Percentage of Drop**
32	1146	25.23

Table 4. Data Packets Analysis

	Normal AODV	**AODV with Black hole and DDOS**	**AODV with Wormhole**
Packet send	5007	2393	4542
Packet Received	4257	633	3705
Packet Drop	750	1760	837

B. Packet Delivery Ratio (PDR) Analysis

The fig. 1 shows the Packet delivery ratio comparison in three cases. PDR is a percentage of data received by the receiver. In this result we show packet delivery ratio at the time of normal AODV without attack, wormhole and black hole-DDOS attack case. The network performance fluctuates under different attack scenario.

Table 4 shows that the AODV gives slightly higher performance than wormhole attack. When black hole-DDOS attack takes place ratio is lower and after 40th seconds whole network is flooded and no data is received by the receiver.

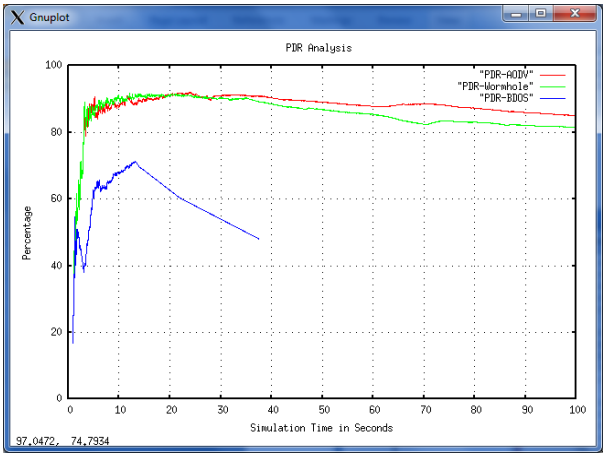

Fig.1. Packet Delivery Ratio Analysis

C. Routing Load Analysis

The fig. 2 shows Routing load of the network. Basically it is a number of search packets broadcasted in the network for establishing communication and routing. This overhead is maximum while network structure is frequently updated or attackers cause mischievous activity in the network. In this graph x-axis shows simulation time in seconds and y-axis number of routing packets spread over the network. The routing loads at the time of AODV and wormhole time are nearly equal. But in the blackhole-DDOS attack case this overhead is very huge because denial of service breaks the route due to network service denial. Results conclude that collaborative blackhole-DDOS attack increases the network overhead due to unwanted data flooding.

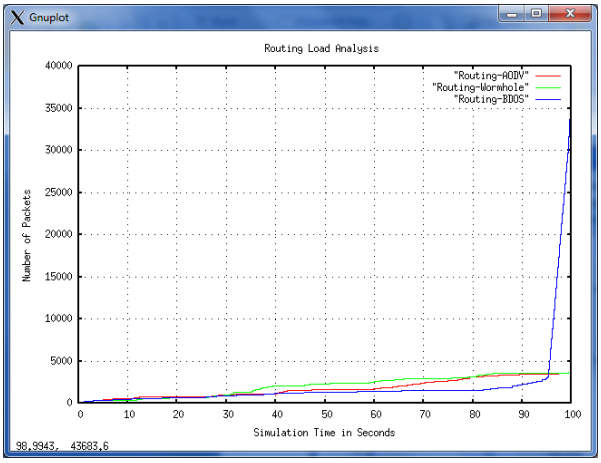

Fig.2. Routing Load Analysis

V. Conclusion

A simple but effective trust evaluation methodology has been proposed to detect different attack typed. The analysis of the generated table helps in identifying wormhole, black hole and distributed denial of service attacks. Simulation studies have been carried out to check the performance of the network with respect of packet delivery ratio, routing load etc. In future, this work can be extended for attack prevention. Different technique can be easily deployed and trained to eliminate malicious nodes in the network to improve the performance of the MANET.

References

[1] H. Yang, H. Luo, F. Ye, S. W. Lu and L Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”,IEEE Wireless Communications Feb, 2004, pp. 38-47, vol. 11, No. 1.

[2] Bing Wu, Jianmin Chen, Jie Wu and MihaelaCardei “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks”, wireless/mobile network security, 2006 Springer.

[3] Neeraj Arya, Upendra Singh and Sushma Singh, “ Detecting and Avoiding of Worm Hole Attack and Collaborataive Blackhole attack on MANIET using Trusted AODV Routing Algorithm”, IEEE International conference on Computer, Communication and Control (IC4), 2015.

[4] H.Hallani and A.Hellany, " Wireless Ad-hoc Networks: Using Fuzzy Trust Approach to Improve Security between Nodes", In International conference on Computer Engineering & System (ICCES’09) Dec-2009, pp. 359-365.

[5] Suresh Kumar, Machha. Narender, and G. N. Ramesh, “Security Provision for Mobile Ad-Hoc Networks Using Ntp & Fuzzy Logic Techniques”, Global Journal of Computer Science and Technology, Sep. 2010, pp. 62, Vol.10, No. 8.

[6] Sakshi Jain and Dr. Ajay Khuteta, “Detecting and Overcoming Blackhole Attack in Mobile Adoc Network”, in International conference on Green Computing and Internet of Things (ICGCIOT) IEEE, June 2015, pp. 225-229.

[7] Farrukh Aslam Khan, Muhammad Imran and Hiader Abbas, “A Detection and Prevention System against Collaborative Attacks in Mobile AD hoc Networks”, Future Generation Computer System 68, 2017, ELSEVIER, pp. 416-417.

[8] Dhiraj Nitnaware and Anita Thakur, “Black Hole Attack Detection and Prevention Strategy in DYMO for MANET”, in 3rd International Conference on Signal Processing and Integrated Networks SPIN, PP. 279-284.

[9] Nitika Gupta and Shailendra Narayan Singh, “Wormhole Attacks in MANET”, in 6th INTERNATIONAL Conference – Cloud System and Big Data Engineering (Confluence), 2016, pp.236-239.

[10] H.VigneshRamamoorthy and Dr.D.Suganya Devi “A New Proposal for Route Finding in Mobile AdHoc Networks “MECS I. J. Computer Network and Information Security, 2013, 7, 1-8.

[11] ParthaSarathiBanerjee, J. Paulchoudhury and S. R. BhadraChaudhuri“Fuzzy Membership Function in a Trust Based AODV for MANET “MECS I. J. Computer Network and Information Security, 2013, 12, 27-34.

[12] Tarunpreet Bhatia and A.K. Verma “Performance Evaluation of AODV under Blackhole Attack” MECS I. J. Computer Network and Information Security, 2013, 12,

35-44.
[13] M.Madhurya, B.Ananda Krishna and T.Subhashini "Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks "MECS I.J.Computer Network and Information Security, 2014, 2, 30-37.
[14] Soumyabrata Talapatra and Alak Roy "Mobility Based Cluster Head Selection Algorithm for Mobile Ad-Hoc Network" MECS I.J. Computer Network and Information Security, 2014, 7, 42-49.
[15] Rakesh Kumar Jha and PoojaKharga "A Comparative Performance Analysis of Routing Protocols in MANET using NS3 Simulator" MECS I. J. Computer Network and Information Security, 2015, 4, 62-68.
[16] Nitin Khanna "Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography "MECS I. J. Computer Network and Information Security, 2016, 4, 37-43.

Authors' Profiles

Ashish Kumar Khare, born in 1977. Ph. D. candidate in SATI Vidisha, Barkatullah University, Bhopal from India. He obtained B.E in Computer science and Engg. From Barkatullah University, Bhopal in 1999. He did his M.Tech form RGPV University, Bhopal in 2007.

In recent years, MANET security has been actively researched. AODV protocol is the elementary problem in identifying trusty routing in MANET. His main research interests include wireless networks and Mobile Ad hoc networks.

Mr. Khare is life member of Computer Society of India (CSI) and ISTE.

Dr J. L Rana, born in 1946. Ph. D. and Ex Professor in MANIT Bhopal from India. He has more than 35 years of experience in research and academics. His main research interests include wireless network and Intrusion detection.

Dr. Rana is life member of Computer Society of India (CSI) and ISTE.

Dr R. C. Jain, born in 1949. Ex Director, Professor and Ph. D. supervisor Samrat Ashok Technological Institute, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal from India.. His main research interests include Data Mining, Image processing and Networking. He has more than 35 years of experience in research and academics. He has more than 80 research paper published in National/International journals and conferences.

Dr. Jain is life member of Computer Society of India (CSI).

How to cite this paper: Ashish Kumar Khare, J. L. Rana, R. C. Jain,"Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.7, pp.29-35, 2017.DOI: 10.5815/ijcnis.2017.07.04