Design and Development of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network

Nilesh N. Dangare
M. Tech. (CSE)
BDCOE

R. S. Mangrulkar
Associate Professor
Head Comp. Engg, BDCE

ABSTRACT
Mobile ad-hoc network (MANET) is used widely today. The work of MANET is totally depends on the cooperation of various nodes in the network. As we compared with the wired network, wireless network has various advantages, such as MANET doesn't require any infrastructure; it is decentralized system and dynamic in nature. Hence MANET is popular in various areas such as Military application, wireless sensor network, Public network and more. But these advantages of MANET may become disadvantages: As its openness, decentralized and dynamic nature, it is highly prone to various attacks. That's why security is the challenging job in MANET. Various existing system for detection of attacks is in-efficient and may require more computation and space as in cryptography technique. In this paper, the focus is given on the Trust based approach to mitigate the attack. In Trust based approach, the most trusted path is selected rather than the shortest path.

Keywords
Mobile Ad-hoc Network, Attacks, Trust based routing.

1. INTRODUCTION
MobileAdhocnetwork(MANET)isoriginallydesignedforacoo perative environment. MANET is a group of wireless mobile nodes that form a network and successful transmission of packet system totally depends on the cooperation of each node in the network. MANET is an infrastructure lessnetwork with each node acts a router andhas processing capability for other nodes. In MANET, there is no geographical limitation; it is a self directed and decentralized wireless system, that's why MANET became popular in various areas, such as military application, sensor networks, some public networks and many more. Due to the open ness and dynamic nature of MANET, it is more prone to various attacks as compared to the wired networks. Packet information is transmitted from source to destination via intermediate nodes. In MANET, routing is heavily depends on various factors, such as, topology, initiation of request, selection of route etc. Malicious nodes can easily disrupt the route discovery during data forwarding phase ,if routing protocol is not secured enough.

Security in MANET is a major aspect in term of packet forwarding and routing. Attacks in MANET can be categories into External attacks and Internal attacks. External attacks are carried out by those nodes which are not part of thenetwork, while Internal attacks are carried by nodes which are the part of the network and more severe and difficult to detect as compared to the External attacks, for example, black hole attacks, wormhole attacks, DOS attacks etc. In Passive attack, the attacker only listen the communication channel to know the confidential information is being transferred without altering or disrupts the operation of the network. The detection of Passive attacks is difficult. In an Active attack, attacker can alters, drop or destroys the data being exchanged.

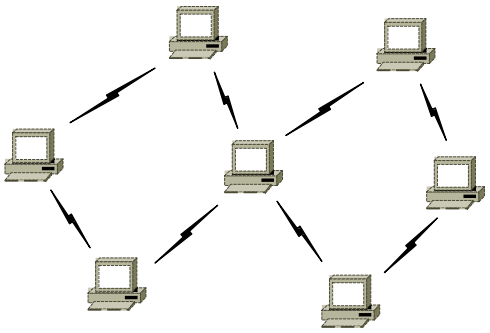

Fig. 1 MANET

The existing routing protocol can be categories into two types Proactive routing protocols and Reactive routing protocols. In Proactive routing protocol (e.g. DSDV), it maintain the routing information all the time and update the routing information by broadcasting the update messages. In volatile environment, due to the information exchange overhead, Proactive routing protocols are not suitable for the mobile ad hoc network. On other side, Reactive routing protocols only maintain the route, which is demanded to reach to the destination. Two widely used Reactive routing protocols are Ad-hoc On Demand Routing (AODV) and Dynamic Source Routing Protocol (DSR). But these two protocols are also affected by various attacks. Normally, Reactive routing protocols having two processes, that is, route discovery and route main- tenance. For providing security, two approaches are popular Cryptographic method and Trust-based method. Cryptographic method provides computational overhead, example SAODV.Trust based method overcome the computational overhead and select the most trusted path rather than shortest path as did in the traditional routing techniques, example TAODV.

2. RELATED WORK
Muhammad Ali et al. [2] Proposed a combine efficient techniques from elliptic curve cryptography and distributed intrusion-detection system (IDS) based on threshold cryptography. The limitation of this scheme is that, it is applicable only to the known attacks. We must have another mechanism to detect newer attacks. Another limitation is that, it added overhead and complexity. The proposed work can be extended through the extension of the current routing protocol by making the communication more secured to protect the routing protocol message.Naveen Kumar et al. [6] Proposed an algorithm which is based on Trust based AODV Routing Protocol for mobile ad-hoc network, and worked on the concept of honest value, which is calculated on the

concept of hop and trust to protect the network from affected nodes (malicious nodes). In proposed HAODV routing protocol, before forwarding the data through various routes, the routing paths have been evaluated according to the trust metrics by the nodes. This method is based on Honest mechanism to secure the AODV routing protocol. The performance of the HAODV has been analyzed using three parameters namely the number of drop packets, throughput and Packet Delivery Ratio. The HAODV performs well in terms of throughput and number of dropped packets. The future work of this method is to implement the proposed scheme with more number of parameters while evaluating the path.

Naveen Kumar Gupta and Amit Garg [9] proposed a Trust based Management framework for securing AODV Routing Protocol. This worked on the concept of Trust factor and selection of most efficient route and using the Trust Value a routing path is evaluated, also during the route exchange process the route gets updated. The performance of the proposed system is calculated based on the Packet Delivery Ratio (PDR), number of drop packets and throughput. The identity information (Internet Protocol address and Trust Factor Value) has been used to prevent the attack by the malicious node. This identity information has been assigned to each node in the initialized phase or when the node has been configured. In future works, to optimize above mentioned scheme in terms of number of nodes and building the fast mechanism to detect and prevent the attacker nodes even when large number of nodes.

Sumathy Subramaniam et al. [12] proposed a framework for Opportunistic Routing help to improve the lifetime of network and Trust model helps to overcome the vulnerability due to attacks by malicious / selfish nodes, to provide reliable packet transmissions. In Opportunistic Routing, one node is selected among the set of candidate nodes as a potentialnext-hop forwarder using metrics like number of transmission in the link, link error probability, cost etc. for the packet transmission. This metrics helps in improving the network lifetime. Also, to prevent attack by malicious nodes, the Trust model is used which is based on direct and indirect Trust degree from similar trusted neighbors. On logical level, a proposed framework for Opportunistic Routing have the Two Modules: Routing Module and Trust Module. Routing module mainly responsible for the selection and prioritization of candidate using the proposed metric, help to improve the residual battery power required for the packet transmission. Trust module is responsible for detection and prevention of malicious and selfish nodes. This Trust module is based on the direct and Indirect Trust degree. As an enhancement to the proposed work, further focus is to determine the delay incurred in transmission of packet from the source to the destination so as to ensure better quality of service in MANET.

Issac Woungang, et al. [13] proposed an enhanced trust based multi-path dynamic Source routing (ETBMDSR) protocol to securely transmit messages in MANETs. Authors proposed a method to improve the TB-MDSR scheme at least route selection time standpoint. The route selection time is the time (measured in seconds) taken by algorithm to find the suitable secured routing path to transmit the message from source to destination. In TB-MDSR scheme [19], a message between source to destination is first broken into four message parts. At the source node, the message parts get encrypted using soft-encryption and similar XOR operation as in [19] (Step 1). The encrypted message parts are transmitted from source to destination through many trusted paths constructed using DSR and selected according to the Greedy approach on a path length basis (Step 2). At the destination node, the received encrypted message are decrypted (using similar XOR operations as in [19]) and the original message is recovered (Step 3). The proposed ETB-MDSR scheme is implemented by following same steps as for the TB-MDSR scheme [19]. However, in Step 2, a new Trust management model [18] is implemented. In ETB-MDSR scheme, History of Interaction (HI) module stores the records on the interactions between nodes in suitable data structure. During trust computation, History Maintenance module is used to maintain and update the History of Interaction(HI) and the Trust Computation module select the coveted entry in the History of Interaction(HI) module, then calculate the Trust value which is based on the direct and indirect Trust values (using Direct Computation and Indirect Computation).

Ahmed M. Abd El-Haleem et al. [15], proposed a novel secure reactive routing protocol for MANET, called TRIUMF for securing MANET against Packet Dropping Attack. It is hard to determine whether the node is malicious or selfish node. This proposed protocol first distinguishes the malicious and selfish nodes and then makes control the degree of selfishness. The proposed monitoring tool first detects the malicious behavior and then the path searchingtool identifies the attacker or compromised nodes in the network and isolated them, and then proposed routing protocol select routes securely. In TRIUMF, AOMDV is used [18], or multi-path DSR to establish two node-disjoint paths between source and destination. But here, the modified RREQ packet is used, containing a list of all unwanted nodes (malicious and selfish nodes), also destination node may have the same list and it may discard all routes which contained this attacker and selfish nodes. Also during the flooding of RREQ, the intermediate nodes will insert the trust rating of previous nodes in the RREQ packet. When the destination node did not receive RREQ packets from intermediate nodes, it select two node-disjoint-paths having the highest path trust value, and certainty factor and then unicasts two RREPs back to the source along with selected two routing paths. In this scheme, authors have used the monitoring tool, including the DLL-ACK and the end to end TCP-ACK to supervise the performance of the routing path. After the misbehaving path is traced out, malicious nodes is to identified with the help of path searching tool and then put the ID's of malicious nodes in the black list to isolated it from the route selection. The future work of this scheme is to compare the result and effectiveness of the solution with the existing trust based routing protocols such as, TAODV, TWOACK and TDSR protocols.

N. Bhalaji et al. [16], Presented a Trust based routing model to deal with Black hole and Cooperative Black hole attacks that are caused by malicious nodes. Here, Author applied the ABDSR (Association based DSR protocol) to route selection to improve the routing security. The purpose of applying ABDSR (Association based DSR protocol) is to determine the foremost and protected route in the network. In this scheme, a Trust value is associated to each node, which represented the value of trustworthiness to each of its neighbor nodes. In proposed scheme, author has classified the association among the nodes and according to the classification, neighboring nodes are categorized into three types: Unknown, Known and Companion.

Unknown: The unknowns are the non trusted nodes, having minimum trust level. When any new node joins the network, its trust relationship with its all neighbors is low or negligible. *Known:* These are the nodes which having the trust value in between the Companion and Unknown. It's means that a node is known to its neighbor node, that is it has received some packets through that node.

Companion: These are the most trusted nodes or the nodes with the highest trust value can be treated as Companion. Means, more the trust level, more the transmission rate through this Companion node (neighbors had received or transfer many packets successfully.)

For calculating the Trust value, author proposed a very simple equation:

$$T = \tanh (R1 + R2 + A)$$

Where,

T is the Trust value.

R1 is the ratio of number of packets actually forwarded by a node to the total number of packets forward that node.

R2 is the ratio of number of packets received form a node but actually originated from others to total number of packets received from it.

A is the acknowledgement bit (0 or 1).

The future scope consist of analyzing the protocol over Gray hole and cooperative Gray hole attacks.

Zen Yan et al. [17], proposed a Trust Evolution based security solution to provide effective security decision on protection of data, safe routing and other network activities. The authors proposed two trust models based on the two ad-hoc system models. One is the independent model that rep-resent independent ad-hoc networks haven't any connection to the predefined (fixed) networks. The second model is the cross model, that represent ad-hoc networks. This model has some few connections to the fixed networks. Personal Trusted Bubble (PTB) represents an ad-hoc node is the basic unit in both models. In PTB, the owner of the ad-hoc device has unreasonable full trust on the device, need for the ad-hoc com- munication and organization. Trust relationship (logical and rational) should be evaluated computationally among bubbles, between bubbles and the fixed networks. The proposed trust evaluation is conducted digitally, ahead of any communication and for the better security decision; the result of this evaluation should be noticed.

3. PROPOSED WORK

In the proposed method, the parameter known as 'Trust Value' is calculated against all the intermediate nodes. This calculated trust value is depending on the ability to forward packets and RREQ forwarding ability of a node. At first number of packets sent, number of packets received, number of RREQ received and number of RREP sent are counted at each link. Then two weight factors are calculated, that is W1 and W2:

Calculate the threshold value W1:

W1 = Number of packets received / Number of packets sent

Calculate the weight factor W2:

W2 = Number of Route request received / Number of Route reply sent

The high value of W1 indicates that, the node has a greater ability to forward the packets. Thus the percentage of packets loss is low. The W2 detects the nodes which continuously receive the RREQ from its neighboring nodes but never give responds to that request by sending the reply that is the silent mode. Thus higher the value of W2 means higher the response of a node, to the route request of its neighbor node. Initially, one base value is assigned to each node that is*ptrust.* This *ptrust* value is increased when threshold value (W1) is greater, otherwise *ptrust* value is decreased. Then the Trust value of each node is calculated as:

Trust Value = W1 * W2 * *ptrust* Value

This Trust Value is inserted into the routing table. Then the most trusted route is established for the data transmission. Rest of the part is similar to the traditional routing protocol.

4. SIMULATION SETUP

For the simulation purpose, NS-2 tool is used. The simulating parameters are as follows:

Table 1 Simulating Parameters

Parameter	Value
ProtocolUsed	AODV
ApplicationTraffic	CBR
PacketSize	512byte
NumberofNodes	10,30,50,150and200
Area	1500*1500m
PauseTime	10s
MaximumSpeed	200m/s
SimulationTime	200s

The normal (nonmalicious) scenarios and malicious scenar-ios have been created. The source node and destination node have been chosen during simulation. The color of source node is set as green and for destination node, it is blue.
Following shows the normal (nonmalicious) scenarios of 10, 30, 50, 150 and 200 nodes.

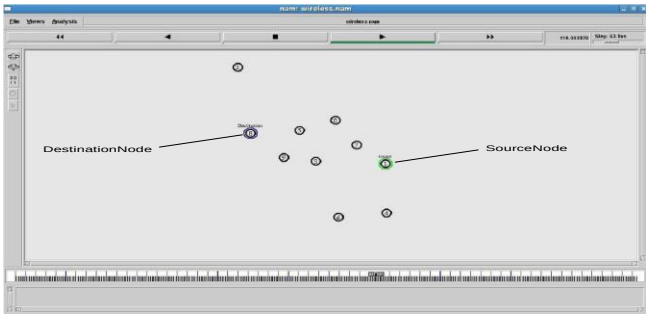

Fig.2 10 nodes

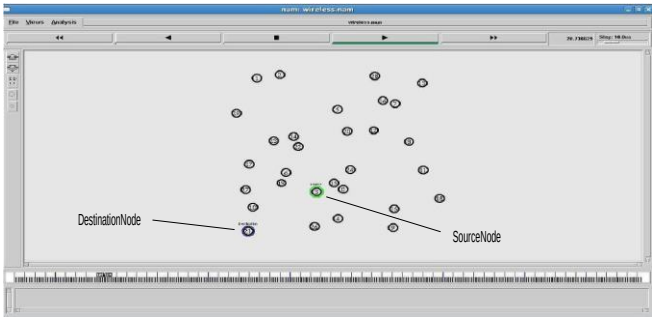

Fig.3 30 nodes

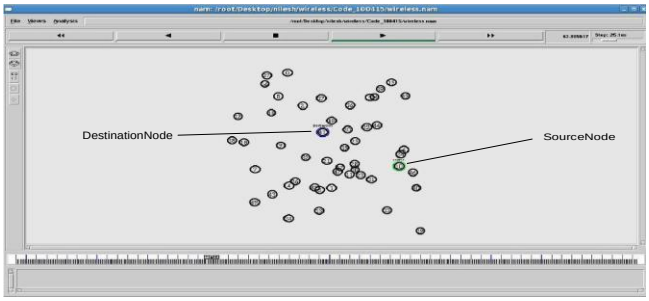

Fig.4 50 nodes

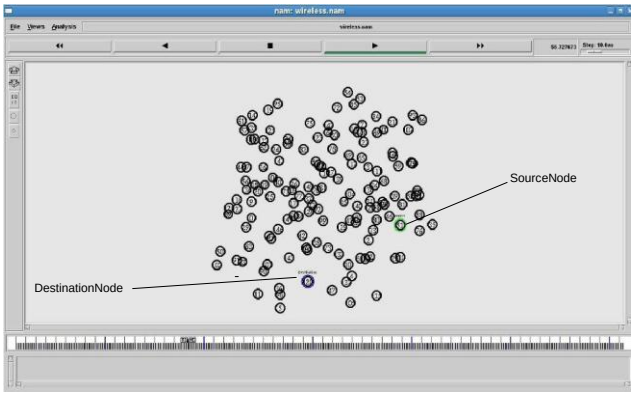

Fig.5 150 nodes

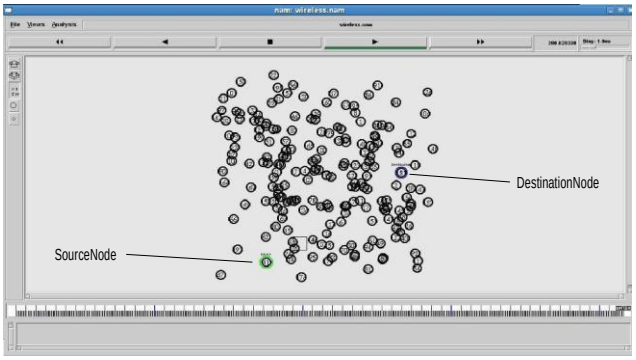

Fig.6 200 nodes

In malicious scenarios, the malicious nodes are generated

randomly. The color of the malicious nodes is set as red. Here, malicious nodes are 10% of the total number of nodes. For malicious node, two files aodv.h and aodv.cc files need to modify. In aodv.h, after:

/* The Routing Agent */ class AODV: public Agent {

.....

/*

History management

*/

.....

Add the following line:

bool malicious;

}

Now make the following changes in aodv.cc file:

1) Initialize the malicious variable with a value"false". Declare it inside the constructor as shown below: AODV::AODV(nsaddr_t id):Agent(PT AODV), btimer(this), htimer(this), ntimer(this), rtimer(this), lrtimer(this), rqueue()

{

index = id;

seqno = 2;

bid = 1;

malicious=false;

.....

}

2) Add the following statement in the "if(argc==2)" statement:

if (strcmp(argv[1], "malicious") == 0) {

malicious = true;

return TCL OK;

}

3) Add the following code in the rt resolve(Packet *p) function to implement the behavior of malicious node: **if(malicious==true)**

{

drop(p, DROP RTR ROUTE LOOP);

}

Once all this done, recompile the ns2:

Open Terminal.

Go to the ns2.35/ directory. (path may be cd /home/user/ns- allinone-2.35/ns-2.35/)

Give the commands:

make clean

make depend

make

Once recompilation is done, add the following line in main tcl file:

$ns at 0.0"[$node ($la) set ragent]""malicious"Following shows the malicious scenarios for 10, 30, 50, 150 and200nodes.

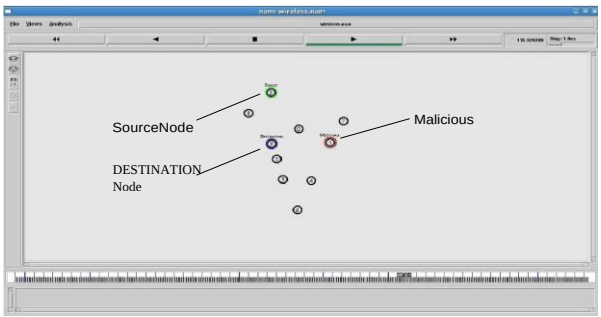

Fig.7 10 nodes including 1maliciousnode

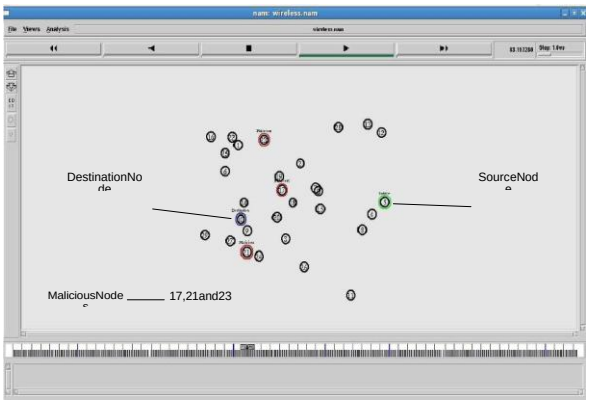

Fig.8 3 0nodesincluding3maliciousnodes

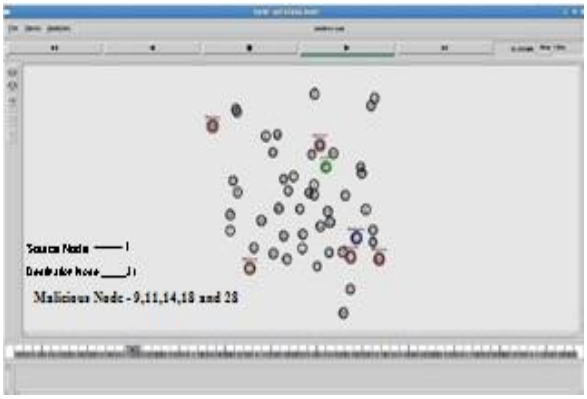

Fig.9 5 0nodesincluding5maliciousnodes

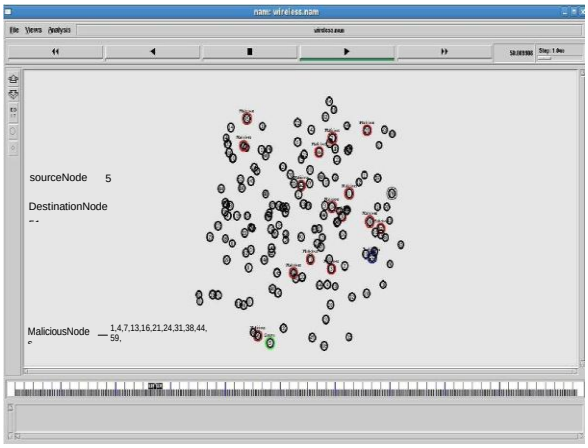

Fig.9 1 5 0 nodesincluding 15maliciousnodes

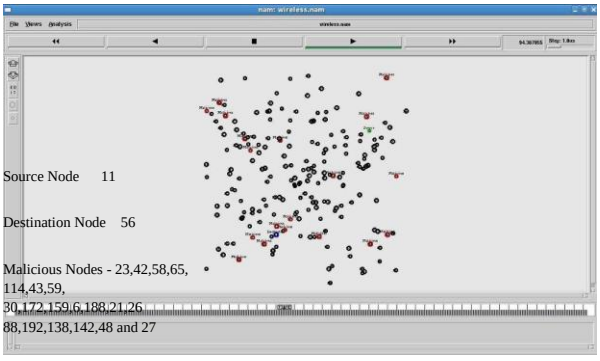

Fig.10 2 0 0 nodesincluding 20maliciousnodes

5. CONCLUSION AND FUTURE SCOPE

The scenarios with malicious and nonmalicious nodes have been created with 10, 30, 50, 150 and 200 nodes. With the help of rand () function, the malicious nodes are generated randomly. The future scope is to implement trust based approach in which the traffic can be passed through the most trusted nodes so that to mitigate the attack and improve the performance of the system.

6. REFERENCES

[1] Pallavi Kharti, "Using Identity and Trust with Key Management for achieving Security in Ad-hoc network", IEEE, 978-1-4799-2572-8/2014.

[2] Muhammad Ali, Subhan Ahmed and Ahsan Mehmood, "Deployment of Security Algorithm in MANETs", IJCCSE, May 2014.

[3] Prof. Ramya S. Pure, Gauri Patil and Manzoor Hussaion, "Trust based solution using counter strategies for Routing attacks in MANET", IJISET, Vol. 1, Issue 4, June 2014.

[4] Poonam Gera, Kumkum Garg and Manoj Mishra, "Trust-based Multi- Path Routing for Enhancing Data Security in MANETs", International Journal of Network & Security, Vol.16, No. 2, PP. 102-111, March 2014.

[5] Prema Jagtap, Seema Ladhe and Sachin Chavan, "Numerous Approaches to Overcome from Black hole Attack in MANET", IJSER, Vol. 5, Issue 2, February 2014.

[6] Naveen Kumar Gupta and Kavita Pandey, "Trust Based Ad-hoc On Demand routing Protocol for MANET", IEEE, 978-1-4799-0192-0/2013.

[7] Deepika Kukreja, Umang Singh and B. V. R. Reddy, "A Survey of Trust Based Routing protocols in MANETs",Journal of Advances in Computer Networks, Vol. 1, No. 4, December 2013.

[8] Priyanka Takalkar and Aaradhana Deshmukh, "Trust Based Secure Data Transmission Model in MANET", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 11, November 2013.

[9] Naveen Kumar Gupta and Amita Garg, "Trust and shortest path selection based routing protocol for mobile ad-hoc netowrks", IJCA, Vol. 76, No. 12, August 2013.

[10] Pallavi Khatri and Aamir Mohammed, "TDSR: Trust Based DSR Routing Protocol for Securing MANET", International Journal of Networking & Parallel Computing, vol. 1, Issue 3, January 2013.

[11] Radha Krishna Bar, Jyotsna Kumal Mandal and Moirangthem Marjit Singh, "Quality of Sservice of mobile ad-hoc network through Trust based AODV routing protocol by exclusion of Black-hole attack", Science Direct, CIMTA 2013.

[12] Sumathy Subramaniam, R. Saravanan and Pooja K. Prakash, "Trusted Based Routing to Improve Network Lifetime of Mobile Ad-hoc Net- works", Journal of Computing and Information Technology, CIT 21, 2013.

[13] Issac Woungang, Mohmmed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao and Chris Liu, "Trust

enhanced Message Security Protocol For Mobile Ad-hoc Networks", IEEE ICC 2012.

[14] N. Bhalaji and A. Shanmugam, "Dynamic Trust Based method to Mitigate Grayhole Attack in Mobile Ad-hoc network", International Conference on Communication Technology and System Design, 2012, 881-888.

[15] Ahmed M. Abd El-Haleem and Ihab A. Ali, "TRIUMF: Trust-Based Routing Protocol with control degree of Selfishness for Securing MANET against Packet Dropping Attack", International Journal of Computer Science Issues, Vol. 8, Issue 4, No. 1, July 2011.

[16] N. Bhalaji and Dr. A. Shanmugam, "Defense Strategy using Trust based model to mitigate active attacks in DSR based mobile ad-hoc network", Journal of Advances in Information Technology, Vol. 2, No. 2, May 2011.

[17] Zhen Yan, Peng Zhang and Teemupekka Virtanen, "Trust Evaluation Based Security Solution in Ad-hoc Networks", 2011.

[18] M. K. Denko, T. sun, and I. Woungang, "Trust Management in ubiqui- tous Computing: a Bayesion approach", Computer Communication, vol 34, Issue 3, pp. 398- 406, 2011.

[19] P. Narula, S. K. Dhurandhar, S. Mishra and I. Woungang, "Security in Mobile Ad-hoc Networks using soft-encryption and Trust based multipath routing", Computer Communication, vol 31, pp. 760-769, 2008.