Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 342 – 349

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

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

Mr. Nilesh N. Dangare[a], Mr. R. S. Mangrulkar[b]

[a]*M.Tech. (CSE), Bapurao Deshmukh College of Engg., Sewagram-442102, Wardha, India*
[b]*Head, Dept. of CE, Bapurao Deshmukh College of Engg., Sewagram-442102, Wardha, India*

Abstract

A Mobile ad hoc network (MANET) is self organizing, decentralized and infrastructure less wireless network. The successful transmission of data packet is depends on the cooperation of each node in the network. These types of network don't have permanent base station, so each node in the network acts as a router. Due to openness, decentralized, self organizing nature of MANET, it is vulnerable to various attacks. So security is the main concern in MANET. In this paper, we considered two attacks; Vampire and DDoS attacks. The Vampire attack is not any protocol specific. Single Vampire attack can increase the network-wide energy usage. DDoS attacks exhaust the resources available to a network. Both the attacks drain the energy of nodes. Here, we discuss method to mitigate these attacks.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: MANET; Vampire Attack; DDoS

1. Introduction

In Mobile Ad-hoc Network (MANET), the transmission of any data packets are totally depend on the cooperation of each node in the network, since packets are transmitted from hop to hop. Also each node has their own transmission range, so if any source node want to send the data packets to the final destination node, source node contact to its neighbour; that neighbour node again contact to another neighbour and so on, so that to reach the final destination node. As we know the wired networks need infrastructure and have centre administration. But in remote location such as mountain, valley, and some public location wired networks are hard to set up. Since MANETs are infrastructure-less, open and no central administration required, it become popular. Today MANETs are widely used in every area where wired networks can not reach. But due to the openness, infrastructure less and dynamic nature of MANET, it is highly sensible to various attacks. In MANET, routing is depends on various factors such as topology,

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.070

selection of route, route requests and responses etc. In MANET, if any attack is occurred, it will affect the whole performance of the network and may some secured information get stolen.

In MANET, to provide the security is the challenging work. Wireless links are more susceptible to various attacks. Malicious behaviour of any node, can disturb the smooth working of any network. To eavesdrop and gain the secrete information are become easy for malicious nodes. Since attackers are more and more intelligent and divers, it becomes hard to provide the security to MANET. Now a day many researchers give focus to develop the new techniques which provide the security to MANETs such as trust based technique.

Attacks can be categorised as Internal Attack and External Attack. External attacks are carried out by nodes which are not part of any network. Internal attacks are carried out by nodes which are in network and more sever and hard to detect as compared to the External attacks, such as Black hole attacks, Gray hole attack, DoS, DDoS, Vampire attack 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. In an Active attack, attacker can alters, drop or destroys the data being exchanged.

This paper is organized as follows: Section I includes introduction of MANET. Section II presents the Literature Survey, including the various techniques to mitigate various attacks. Section III introduces the types of attacks. In this paper, the vampire attack and DDoS attack are into consideration. Section IV presents the Propose Work. Section V presents Result analysis and Section VI presents Conclusion and Future scope.

2. Literature Survey

Sandeep A. Thorat and P. J. Kulkarni[2] compared trust based and cryptographic approaches for implementing security in MANET routing. Author discussed the design issues in trust based routing protocol for MANET in details. Paper has been presented a survey on trust based routing protocol and provide directions for future research in trust based routing protocol for MANET.

Ramya S. Pure et al[5] suggested proposed model which is designed over the ad-hoc On-demand distance vector routing protocol (AODV). The proposed routing algorithm adds a field to store the trust value or node's trust on its neighbor, so that the computational overhead can be reduced and trustworthiness of routing procedure can be generated. Based on the trust value of node, the routing information will be forwarded to the next node having highest trust value. Authors also worked on the some attacks such as Black hole attack, Gray hole attack and Wormhole attack. The proposed method helps to improve the throughput of the network.

Naveen Kumar Gupta and Kavita Pandey[7] 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 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[8] 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.[11] 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 potential next-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 has 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.[12] 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[10], 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[10] (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[10]) 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[10]. However, in Step 2, a new Trust management model[9] 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.[13] 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 searching tool 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[9], 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.

Zen Yan et al.[15] 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 represents independent ad-hoc networks, have not 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 adhoc device has unreasonable full trust on the

device, need for the ad-hoc communication 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. Attacks

Security is the main concern of any MANET for secure transmission of any data. Due to the decentralized and open nature of wireless system, MANET is highly prone to various attacks. Attacks can be categorised as *Passive attacks* and *Active attacks. Passive attacks* only monitor the data traffic and looks for clear text password and other sensible information which may be used in other attacks. *Active attacks* try to break the security system. Active attacks may include introducing malicious nodes, to steal or modify the sensitive information and break or bypass the security mechanisms. Types of attacks are as follows:

- *Black hole Attack:* In this type of attack, malicious nodes broadcast the message to all the nodes, that it has valid, shortest and fresh route to the destination. In this way, such malicious nodes divert all the traffic toward itself and without forwarding the data packets to the neighbouring nodes, all the data packets are dropped.
- *Gray hole Attack:* This attack can be considered as a form of Black hole attack. In this type of attack, the malicious nodes drop the data packets for particular nodes for particular period of time in the network. That is why Gray hole attack is more difficult to identify as compare to the Black hole attack.
- *Wormhole Attack:* In this type of attack, two malicious nodes form a tunnel and all the data packets received at one location of the network are tunnelled at other location in the network. in such way all the data are resend to the network. the tunnel between two malicious nodes is called as Wormhole. Such attacks prevent any route other than through the wormhole from being discovered.
- *Byzantine Attack:* This type of attacks is carried out by intermediate nodes or group of intermediate nodes. Such malicious nodes provide the false routing information and create routing loop as well as forward the data packets to that path which is not optimal which may harmful to the routing system.
- *Denial of Service Attack:* It prevent the victim from being used all or part of the network connections. DOS attack may have numerous forms and hard to detect. In this type of attack, attacker nodes send the excessive amount of data packet or request to the server so that server get busy in testing illegal request and will not be available to the other. This attack may degrade the performance of the network since it consume the the energy (Battery Power) of nodes.

In this scenario, the two attacks are considered: *Vampire Attack* and *DDoS Attack.*

Vampire Attack: This is not protocol specific attack and hard to detect. This attack may exploit general properties of protocol classes such as link-state, distance-vector, source routing and geographic routing[6]. It drains the power of node which may result in network failure and data loss. The attacker packets (Vampire packets) consume more power of any node than the normal packets.

DDoS Attack: This can be carried out from several layers. it is a distributed, large-scale attempt by malicious nodes to amass the victim network with an enormous number of packets. This exhausts the resources of victim network, such as bandwidth, computing power etc. In such case, victim unable to provide the services to its clients and network performance may degrade. DDoS attack can be categories as Volumetric Attacks, TCP State- Exhaustion Attacks and Application Layer Attacks.

4. Proposed Work

In the proposed work, the cluster based network is formed. Ten nodes are considered in each cluster. Total number of cluster is based on the total number of nodes in the network. Two nodes having maximum energy have been selected in each cluster.

Selection of Cluster:

Max _Cluster = expr [val (nn) / Max_Node_ in_ Cluster]

Here, val (nn) is the total number of nodes in the network and maximum ten nodes are considered in each cluster. Also X and Y coordinates (Maximum values of X and Y) have been calculated for each cluster:
*set max_ x [expr [expr $CURRENT_CLUSTER + 1] * $val (x) / $MAX_CLUSTERS]*

To calculate the energy of node, rand() function is used. The two nodes with highest energies in each cluster have been calculated. These two nodes are called Cluster Head 1 and Cluster Head 2. In between Cluster Head 1 and Cluster Head 2, node with highest energy is selected as CLUSTER HEAD in each cluster.

4.1 Proposed Design

The basic idea behind the trust based approach is to find out nodes having highest energy. In each cluster of network, maximum two nodes are identified having highest energy called trusted nodes. The communications are carried out through these trusted nodes. That is trusted node in each cluster send the received packets to the destination or next trusted node in another cluster and so on. To find out the malicious nodes in the network, send and received packets as well as route response is calculated. Then the number of packets (send & received) is compared to the threshold value, if it is less than the threshold value then particular node is considered as a malicious node.

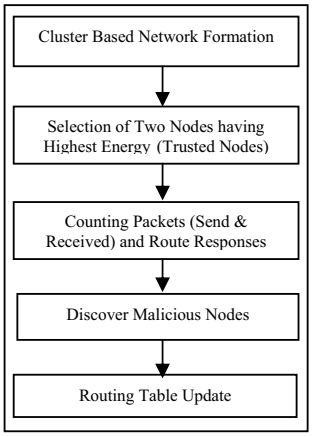

Figure 1: Work Flow

4.1.1 Cluster Based Network Formation: The number of cluster is depends on the total number nodes in the network. Here maximum number of nodes in the cluster is considered as 10. To place the node in the cluster, the value of x and y coordinates of each cluster are determined to make sure that each x and y coordinates of each cluster within the specified range. For example for a network of 300m x 300m, if the numbers of clusters are 3 then each node will be placed in 100m x 100m area.

4.1.2 Selection of Trusted Nodes: After formation of the network, the trusted nodes are determined (Nodes having highest energy). To choose the random energy of each node, rand () function is used. For example, expr rand ()*1000. We can also check the energy of each node by using, set e [$node (2) energy]; then print the value of e. After calculating the initial energy of each node in each cluster, nodes with highest and second highest energy have been chosen. These two are called as trusted nodes in each cluster. These nodes with highest and second highest energy are referred as cluster head one and cluster head two respectively. All the communications will be carried out using these cluster heads.

4.1.3 Counting of Packets (Send & Received) Along with Route Responses: The send and received packets are calculated for each node; also route response of each node is determined. This information is helpful to determine the malicious node in the network. Node having less route response and send packets may be considered as a malicious node.

4.1.4 Comparison of Packets with Threshold to get Malicious Node: To get the malicious node, the number of packets (send & received) is compared with the threshold value to determine the malicious nature of any node. While calculating, the route response is also taking into consideration. The Threshold value is set as 30. Here, we take into account the DDoS attack. This comparison is playing a vital role to determine the DDoS attacks. The figure 6 shows the detection of malicious nodes.

4.1.5 Routing Table Update: After determining the trusted nodes and malicious nodes in the network, the information is updated in the routing table. According to the routing table, most trusted path is selected for communication which helps to improve the network life as well as network performance.

5. Result Analysis

For the simulation purpose Network Simulator 2 (NS-2.35) has been used. Simulation parameters are as follows: The simulation area is 300 m by 300 m. AODV protocol has been used, since AODV protocol is loop free, avoid counting to infinity problem and does not need any central administration system to handle routing process. The UDP is used as application traffic. UDP has two advantages over TCP: First, the source node continuously sends UDP packets even if malicious nodes drop them, while node finishes the connection if it used TCP. Second, it is able to count sent and received packets separately even if UDP connection is lost during simulation; but in case of TCP, node finishes the TCP connection after a while if it has not received the TCP acknowledgment packet. Following are simulation parameters:

Parameters	Value
Simulation Area	300 * 300
Number of Nodes	30
Routing Protocol	AODV
Application Traffic	CBR
Packet Size	1000 byte
Simulation Time	(Total No. of Nodes + 3) Sec
Packet Interval	0.07 Sec
Queue	50

Table1: Simulation Parameters

Figure 2 shows creation of normal scenarios. Here, we can see the communications are carrying out between Node 4 & Node 15 and Node 5 & Node 16.

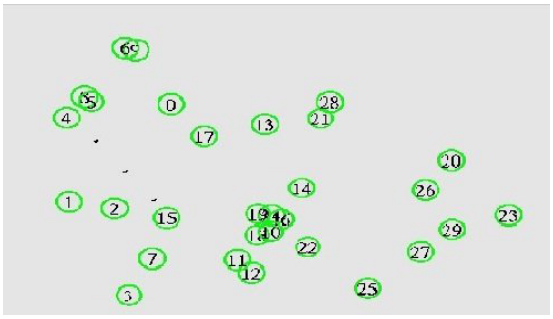

Figure 2: Normal Scenario Creation

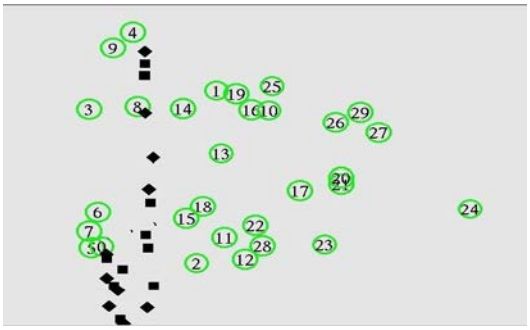

Figure 3: Scenario with DDoS Attack

Figure 3 and Figure 4 show the scenarios with DDoS and Vampire attacks respectively. It shows the packets get

dropped (DDoS attack) between Node 4 & Node 15 and Node 6 & Node 17 and Node 18 is affected by Vampire attack.

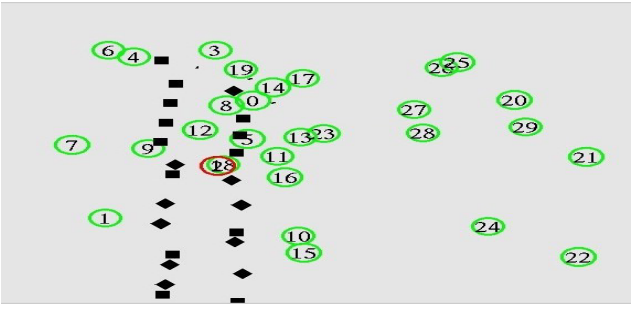

Figure 4: Scenario with Vampire & DDoS Attacks

Following Figure 5, Figure 6, Figure 7, Figure 8, Figure 9 and Figure 10 shows the PDR, Throughput, Goodput, Delay, Jitter and Energy respectively.

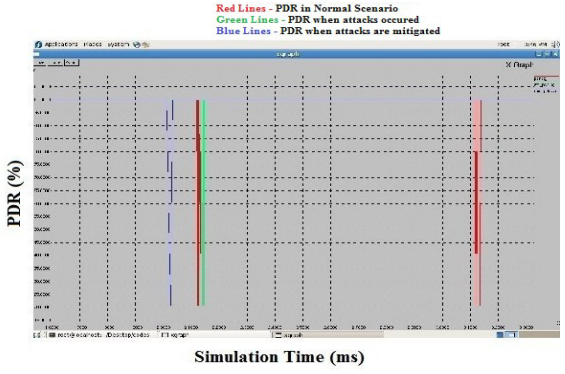

Figure 5: Packet Deliver Ratio

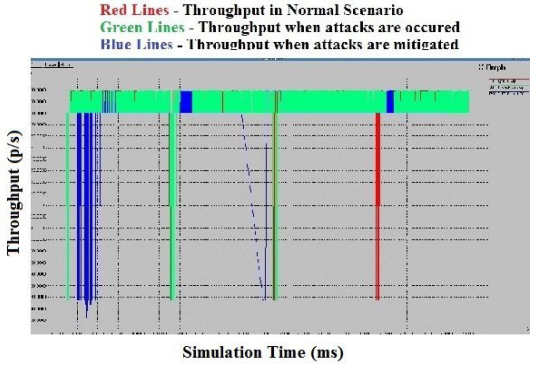

Figure 6: Throughput

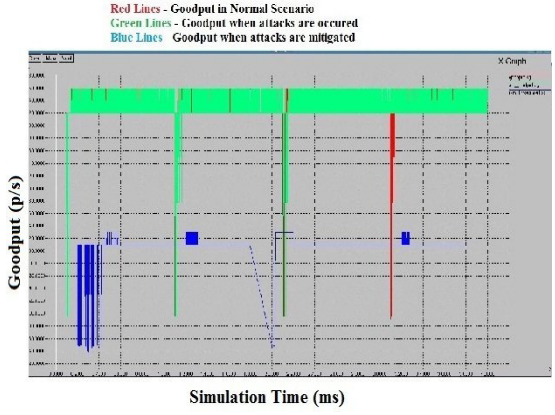

Figure 7: Goodput

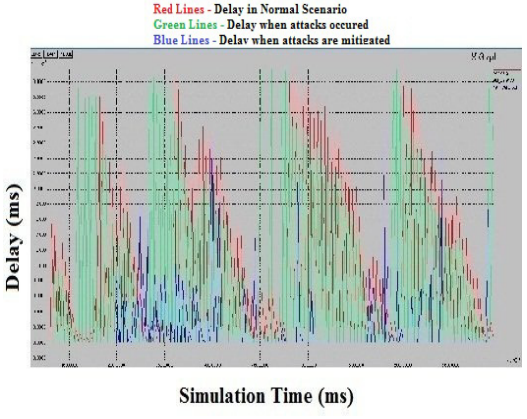

Figure 8: Delay

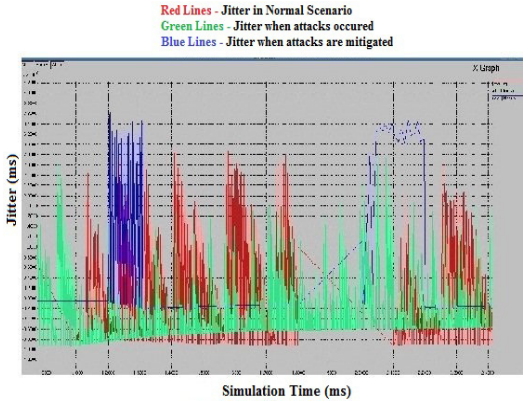

Figure 9: Jitter

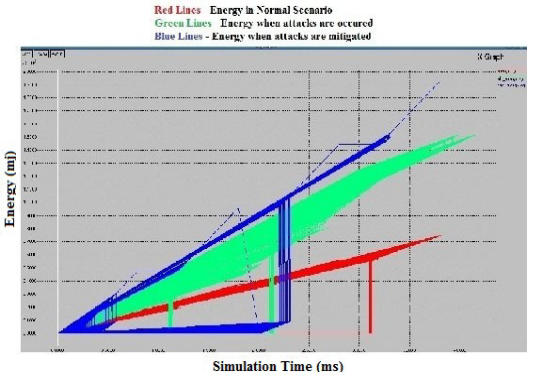

Figure 10: Energy

6. Conclusion And Future Scope

The Vampire and DDoS attacks are resources consumption attacks which drain the energy of node in the network. If energy of nodes drain, packets forwarding process may affect which may degrade the performance of the network. Here we consider small network of 30 nodes which are divided into three clusters; each cluster included ten nodes. Simulations have been performed and various parameters have been considered. From the result, we can conclude that the Vampire attack and DDoS attack have been mitigated using trust based approach. The future work is to use the proposed technique to mitigate Vampire and DDoS attacks with more number of nodes and increasing the simulation area and also for other types of attacks.

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. Sandeep A. Thorat and P. J. Kulkarni. *Design Issues in Trust Based Routing For MANET*; IEEE; July 11-13, 2014.
3. Jenitha T. and Jayashree P. *Distributed Trust Node Selection for Secure Group Communication in MANET*; IEEE; 978-1-4799-4363-0/2014.
4. H.Bharani, M.Kanchana, S.B.Dhivya, V.Kavitha and I.Vinnarasi Tharania. *Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Network;* IJSTE; Vol. 1, Issue 1, July 2014.
5. Prof. Ramya S. Pure, Gauri Patil and Manzoor Hussaion Hussaion. *Trust based solution using counter strategies for Routing attacks in MANET*; IJISET; Vol. 1, Issue 4, June 2014.
6. G. Vijayanand and R. Muralidharan. *Overcome Vampire Attacks Problem In Wireless Ad-Hoc Sensor Network By Using Distance Vector Protocols;* IJCSMA; Vol. 2, Issue. 1, pg. 115-120, January- 2014.
7. Naveen Kumar Gupta and Kavita Pandey. *Trust Based Ad-hoc On Demand routing Protocol for MANET* ; IEEE; 978-1-4799-0192-0/2013.
8. Naveen Kumar Gupta and Amita Garg. *Trust and shortest path selection based routing protocol for mobile ad-hoc networks*; IJCA; Vol. 76, No. 12, August 2013.
9. 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.
10. 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.
11. Sumathy Subramaniam, R. Saravanan and Pooja K. Prakash. *Trusted Based Routing to Improve Network Lifetime of Mobile Ad-hoc Networks*; Journal of Computing and Information Technology; CIT 21, 2013.
12. 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.
13. Ahmed M. Abd El-Haleem and Ihab A. Al. *TRIUMF: Trust-Based Routing Protocol with control degree of Selfishness for Securing MANET against Packet Dropping Attack*; International Journal of Computer Science; Vol. 8, Issue 4, No. 1, July 2011.
14. 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.
15. Zhen Yan, Peng Zhang and Teemupekka Virtanen. *Trust Evaluation Based Security Solution in Ad-hoc Networks*; 2011.