International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||5||Pages|| 2874-2879||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Detection Techniques for Sybil Attack in MANETs

Shamikh Faraz
M. Tech final semester, Dept. of Computer Sc. & Engineering,
Uttrakhand Technical University, Dehradun (U.K.)
shamikh.faraz@hotmail.com

Abstract: For detection of a Sybil attack, a traditional method defenses against attacks rely on trusted identities provided by a certification authority, but requiring users to present trusted identities run counter to the open membership that underlies the success of these distributed systems in the first place, but this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. There are also two other approaches to detect the Sybil attack, one is Lightweight Sybil Attack Detection Approach and other is Robust Sybil Attack Detection Approach. Also some other techniques are discussed in research paper.

Keywords: detection mechanism, robust detection, lightweight detection, Sybil attack detection**.**

1. Introduction

Mobile ad -hoc network (MANET) is an independent network which consists of many nodes and these nodes use wireless links to communicate with each other. A mobile ad hoc network due to its open nature, dynamically changing topology, lack of infrastructure and central management is vulnerable to various attacks. There is an attack which causes many serious threats to the network and it is known as Sybil attack. In other words a '**Sybil attack'** in network security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. In this, attackers use many identities or IP addresses to gain control over the network and creates lots of misconception among nodes present in the network. Malicious attackers can create multiple identities and influence the working of systems that rely upon open membership. Examples of such systems range from communication systems like email and instant messaging to collaborative content rating, recommendation and delivery systems.

A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links, to form an arbitrary topology. The movement of the nodes in MANET is random. Thus the topology of the wireless network may change unpredictably and rapidly. There is no central governing authority in MANET, so the nodes act as hosts as well as routers. Routing has to be enabled in each node to provide the routing service. Nodes in the MANET are equipped with wireless transmitters and receivers using antennas. The antennas may be Omni-directional or broadcasting, highly directional or point to point which may be steerable or a combination of these. MANETs have many salient features such as dynamic topology, bandwidth constrained applications, energy constrained operations and limited physical security.

1.1 Dynamic Topology

The movement of the nodes in MANET is arbitrary and hence the topology of the network may change rapidly and randomly at unpredictable times which in result may contain both unidirectional as well as bidirectional links.

1.2 Bandwidth Constrained applications

Nodes in the MANET are having limited bandwidth constrained and have lower link capacity than the traditional wired networks. The maximum transmission rate of a node is always lowered due to various factors in the network like multiple access, fading, noise and interference etc. Some application like multimedia computing and collaborative networking demand more bandwidth which may sometimes exceeds the network capacity. The main characteristics of MANETs are

1.3 Energy Constrained operations

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the operations should have optimized design criteria for conserving energy.

1.4 Limited physical security

Mobile ad hoc Network is more vulnerable to security threats than the traditional wired network. The attacks such as eavesdropping, spoofing and denial of service are rapidly growing and must be taken into consideration. Some of the security techniques available for the wired network are also applied to the MANET for reducing the threats and the decentralized nature of the network topology in MANET helps network to be more robust against single point of failure that is in the case of a wired network. The task of making a network scalable and preventing it against the security threats at same time is very difficult.

2. Detection mechanism

In the mobile environment, a single entity impersonating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range. Assuming an attacker uses a single-channel radio, multiple Sybil identities must transmit serially, whereas multiple independent nodes can transmit in parallel. The identities established by a Sybil attacker whether represented by IP addresses, MAC addresses, or public keys differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple identities, any

particular assumed identity is resource constrained in computation, storage, or bandwidth.

Though there is no general, universally-accepted solution to the Sybil attack, a number of approaches for various combinations of environments and attacks have been proposed. Some methods mitigate the threat level of these attacks in a system to a satisfactory minimum without incurring an appreciable performance overhead. We must note that although they will not completely eliminate the possibility of the attack occurring, they are more than worthy of consideration.

Notable techniques to counter Sybil attacks are as under.

S. No.	Mechanism Name	Architecture	Summary
01	Lightweight Sybil Attack Detection	Distributive	The nodes entering in the network with speed greater than the threshold speed are detected as Sybil nodes.
02	Robust Sybil Attack Detection	Distributive	The nodes having the same path or pattern are detected as Sybil nodes.
03	Secure Address Allocation	Distributive	The Sybil attack is prevented as Unique addresses are allocated to each node in the network.
04	Received Signal Strength based	Distributive	Plot the RSS of nodes in order to determine and visualize the behavior of the new legitimate nodes and the Sybil attackers

Table 1: Sybil attack detection techniques

3. Lightweight Sybil attack detection technique

In this, each node collects the information about the RSS value of neighboring nodes. On the basis of RSS value, distinction can be made between legitimate and Sybil nodes. If the RSS value of the new node which joins the network is low, then that node is considered as legitimate node otherwise it is considered as Sybil node.

Received RSS
Passed to addNewRSS (Address, rss,time_recv) function
Address is not present in RSStable
It implies that it is a new node
Now its RSS value is compared withUB_THRESHOLD valuerss>=UB_THR
ESHOLD
Address is added to RSS table anddetected it as a legitimate node
Address is added to the malicious node list

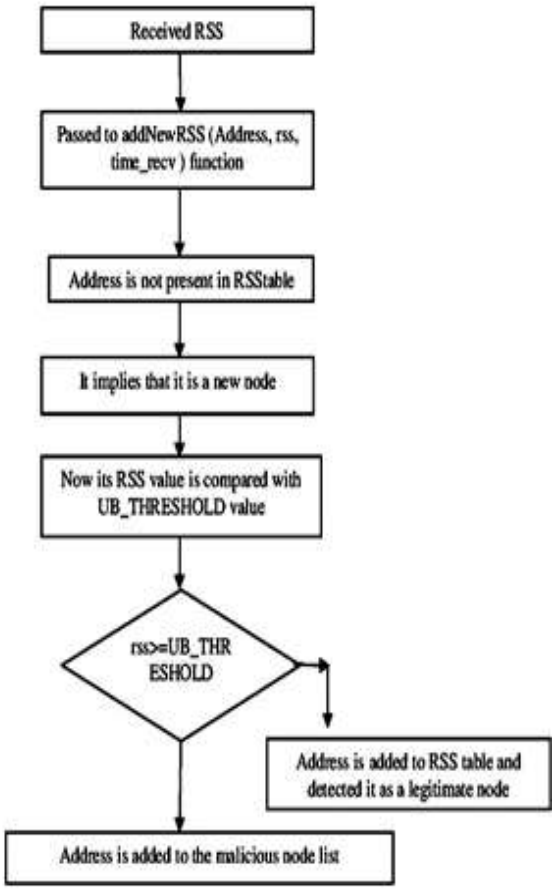

Figure 1: Lightweight Sybil attack detection

3.1 Exposure of Sybil nodes

In this, assumption is made that no legitimate node can have speed greater than 10m/s which is called as threshold value or threshold speed. On the basis of speed, RSS value is calculated and if the RSS values of nodes are greater than or equal to threshold value than those nodes are detected as Sybil nodes otherwise as legitimate nodes.

3.2 Algorithm explanation

In this the received RSS value of node is passed to the addNewRSS function and then address of that node is checked that if it present in RSS table or not, if it does not present in RSS table then node is considered as new node. Now RSS value of new node is compared with the upper bound threshold value, if RSS value of new node is greater or equal to upper bound threshold value then it is detected as malicious node otherwise detected as legitimate node.

4. Robust Sybil attack detection technique

This is another technique used to detect the Sybil nodes. To implement this technique, some methods are required forth correct observation of traffic. These methods are discussed below.

1. Robust Sybil Attack uses the authentication mechanism for the traffic observation. In this, each packet is designed by the sender's private key and also signed by the nodes which are traversed by it to reach the destination and in the end receiver authenticate it by its public key. So, it gives the proof that at what time and location sender sends the packet and in which direction the packet is send by the sender, so that it will reach to the destination.

2. To check the similarity of the path, it uses the novel location based Sybil attack detection mechanism. The nodes whose path is exactly similar to each other are detected as Sybil nodes. The similarity of the node's path is checked by their overlapping components that how much they are overlapped. The similarity of the path is checked as follows.

Sim(L1,L2)=
HereL1, L2 are nodes
Tobs1= It is a duration when each node is observed.
Tbobi= It is a duration when both nodes are observed in the observation table.
Tcoi= It is a duration when both nodes are observed at the same time and they co-exist in same area.
j= It is the number of times when both nodes are observed commonly

The first part of equation is used to calculate that till what time both nodes are observed commonly and second part of equation is used to determine the overlap region of the nodes.

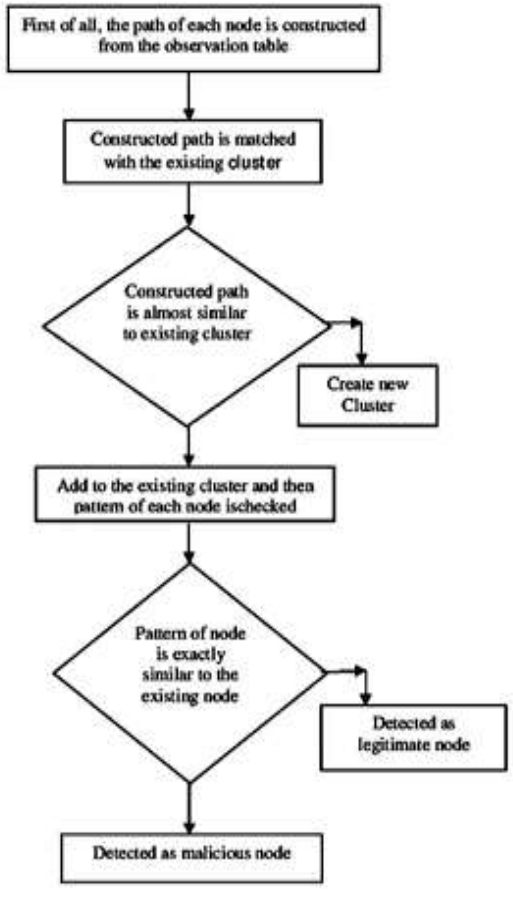

Figure 2: Robust Sybil attack detection

5. Prophet address allocation technique

To allocate unique IP address to the nodes, it uses a partition function f(n) which is used to generate sequence of integers. Here partition function is based on fundamental theory used in number theory. The partition function is also called the state function which is associated with the beginning state or node called seed. These seeds are used to generate different sequence of integers. These sequences should consist of following characteristics:

a) There should be a long gap between the numbers which is repeated again in the sequence.

b) The likelihood occurrence of the same number again in a sequence should be very less.

As number or integer calculation includes the allocated address or the addresses which has to be allocated, by following above two characteristics it escapes the battle among the occurrence of same IP address again. The disadvantage of prophet address allocation is that seed value remains same throughout the network, so it is possible for the malicious node to come to know about the seed value by acting as a new node and causes various attacks in the network like IP spoofing, State pollution and Sybil attack.

5.1 Secure Prophet Address Allocation

It is an advanced version of prophet address allocation.

a) *Authentication of seed value:* The value which is generated by the initial node in the network is called seed value. During the allocation of address to the nodes, the seed value remains same throughout the process. When a new node enters in the network, first of all it must be authenticate that it receives the seed value from the legitimate node but as the seed value remains same throughout the network so it is difficult to authenticate that seed value doesn't come from malicious node. So to get the unique address in the network, it depends upon the uniqueness of the exponential array which is explained in next step.

b) *Improvement*: In the prophet address allocation updates are done within the states when the address is allocated, and in secure prophet address allocation when the address is allocated, updates are flooded in the entire network. In this, acknowledgement consists of four variables that are seed value, index of increasing exponential, exponential array, priority variable and the source address of the responder.
c) Exponential array: In this new node inherits the parameter from its ancestors to calculate its own address. Exponential array variable tells the relationship between the new node and its ancestors.
d) Priority Variable: The greater number represents the newness of the state and greater the number, the more priority state will have. The new node will choose the high state priority number variable and then add some arbitrary value to its priority to calculate its own address. When the address is calculated then it floods the acknowledgement about the priority variable in the entire network. All nodes in the network update their priority values.
Relationship among the variables is following:

X= f(a, i[1..n])
Where X= Source address of the responder

a= seed value
c= index of exponential
p= priority
i[1..n]= Initial exponential array
r= arbitrary value select by the new node
Address of new node (y) is calculated as follows: y= f(a, e[1..n]) where i[j], j<c e[j]= p+r, j=c [3] i[j]=0, j>c

By using above formulas, distinct addresses are computed for all new nodes. In this each node has unique address and no node will use each other's address for an attack, so like this it will prevent Sybil attack.

6. RSSI based detection technique

We will setup our detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from new comers, if greater than the threshold imply abnormal entry into the neighborhood. Now the question becomes, which speed should we adopt as the upper bound for our detection threshold fromFig.4.3 determining node presence with respect to different speeds.

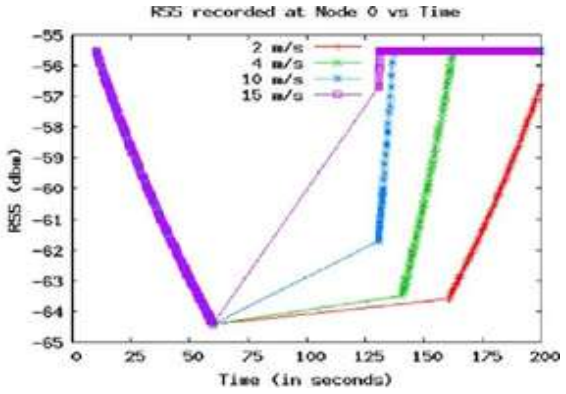

Figure 3: RSSI based detection

To answer this question and for clarity purposes, logically partition the radio range of node *A* into two zones: a gray zone and a white zone. Please note that this partitioning is based on the speed-based detection threshold. If I incorporate various speed-based thresholds from Fig. 4.3, it would become clear that higher speed thresholds produce wider gray zones. Whitewashing in this area cannot be detected, since the first appearance (or acknowledgment) of a node in the gray zone would usually represent a normal entry into the radio range of the node. We used 10 m/s as an upper bound speed because we believe that in most of the ad hoc network applications including vehicular ad hoc networks in urban or congested areas, nodes usually may not move faster than 10 m/s (36 km/h) that is why we choose it to be a good upper limit for our scheme. So any new identity creation in the white zone will be detected as a whitewashing or Sybil identity, because normal nodes cannot produce their first appearance in this area. From the above discussion, we can deduce that smaller speed-based thresholds will work better than larger ones because they will produce high true positives. Please note that we adopt a 10 m/s threshold in our simulation based evaluation in Section VI, and for this speed the simulation produced sound results. We believe that detection will be improved by using a lowers peed threshold than 10 m/s. For example, if in a network the maximum speed of nodes is 2 m/s then the detection threshold based on this speed would produce narrower gray zone, hence detection accuracy will be improved. The problem is that a good node with very low in/out traffic can incorrectly be detected as a Sybil attackers' new identity when it silently appears in the white zone of nodes. For example, suppose *C* is the destination-only node in the white-zone of node *A* (node *A* is not aware of node *C*), and currently

C is not receiving any traffic from its source node due to the connection being broken (due to mobility or other reasons) and that it has not re-established a connection yet. Node *A* will detect *C* (being a good node) as a whitewasher when node *C*'s previously broken connection is re-established, resulting in a false positive. One way to reduce such false positives is th at each node should transmit periodic beacon messages in order to indicate their presence; however this generates substantial communication overhead in the network. A promising solution to mitigate this issue is that each node should promiscuously listen (overhear) to each data and control frame transmitted in the network. Since in ad hoc networks nodes forward packets for each other, a node having no connection(s) to/from other nodes can still transmit ample number of data and control frames to show its presence, when acts as a forwarder. Hence, overhearing these frames will decrease such types of false positives, a fact we will demonstrate in our simulation results. We have shown the natural behavior of new entrants. Now node *A* can easily differentiate between a new node *B* that is coming into its neighborhood and an identity created by a Sybil attacker, pretending to be a new node joining the neighborhood. This is done as follows. Node *A* will make a decision based on the RSS values of the nodes. If the first RSS value captured is greater than the threshold, i.e., a node is in the white zone, *A* will deem that identity as a new identity from a Sybil attacker, since no node can penetrate into white-zone within the specified speed. If the first RSS value received is less than the threshold, i.e., a node is in the gray zone, it will be considered as a normal new entrant and will be added to the neighbor list. Upon detection of Sybil identity, the detector node will inform its 1-hop neighbors by transmitting a special *detection update* packet. Each node when receives two or more than two packets from two distinct nodes about an identity to be Sybil, that identity will be deemed as Sybil identity. There are two issues in the above detection mechanism. First, what will happen to a legitimate node that switch of fits transmitter or device in one neighborhood and turn it on in another neighborhood? The possible solution would be that since good nodes usually try to preserve their identities; they will reveal their identities on each emergence. Nodes sharing good nodes' identities list in the network, will easily find the existing nodes' appearances in the network. Second, what will happen when a Sybil attacker varies its transmission power to mimic arrival from a distance? The answer to the above issue is that to the best of our knowledge, practically it is very difficult to achieve these using current off-the-shelf cards as pointed out by [22].In order to detect new identities spawned by a white washer or Sybil attacker, Algorithm 1 checks every received RSS by passing it to the addNewRss function, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with before, i.e., it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an *UB−THRESHOLD* (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e., whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list.

Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it. Finally, the size of the link list is checked, if it is greater than the *LIST−SIZE*, the oldest RSS is removed from the list.

7. Reputation System

For many p2p systems, including ad hoc networks and online markets, reputation systems have received a significant amount of attention as a solution for mitigating the effects of malicious peers. In an important work, **Cheng** and **Friedman** evaluated the vulnerability of reputation systems to the Sybil attack, classifying them as **symmetric** or **asymmetric** approaches.

7.1 Symmetric Reputation

A symmetric reputation system is one in which an identity's reputation depends solely on the topology of the trust graph, and not the naming or identity of nodes. An attacker that wishes to increase its reputation simply uses Sybil identities to create a copy of the existing graph representing trust relationships. A symmetric reputation system cannot distinguish original nodes from the copies, and thus some Sybil node has reputations equal or better to any original node.

7.2 Asymmetric Reputation Systems

In asymmetric reputation systems, there are specifically trusted nodes from which all reputation values propagate. Alternatively, each entity separately computes a trust value along their unique paths to every other identity in the system. Since the trusted nodes cannot be impersonated, no Sybil attacker can create a duplicate graph as explained in the symmetric case. This trust value can change over time as the entity interacts with and observes the behavior of different identities. Asymmetric reputation systems can be effective at raising the cost of Sybil attacks because attackers are forced to build up trust before effectively launching attacks. Unfortunately, these systems inevitably penalize newcomers who must prove themselves by offering benefits before getting anything in return.

7.3 Role of Reputation System

Reputation systems can be used to cope with any kind of misbehavior as long as it is observable. The goal of reputation system is to enable nodes to adapt to changes in the network environment caused by misbehaving nodes. This is achieved by the following functions.

Monitoring

Reputation

Response

7.3.1 Monitoring

Monitoring systems detect misbehavior that can be distinguished from regular behavior by observation. Nodes can automatically learn about new misbehavior in analogy to the human immune system.

7.3.2 Reputation

The terms reputation and trust have been used for various concepts, also synonymously. Reputation here is to mean the performance of a node in participating in the base protocol as seen by other nodes. For mobile ad hoc networking this means participation in routing and forwarding. By trust we mean the performance of a node in the policing protocol that protects the base protocol, here reliability as a witness to provide honest reports.

7.3.3 Response

Detection and reputation systems aim at isolating nodes that are deemed misbehaving by not using them for routing and forwarding, and most also isolate them additionally by denying them service.

7.4 Features of a Reputation System

7.4.1 Representation of Information and classification

These determine how monitored events are stored and translated into reputation ratings, and how ratings are classified for response. Use of second-hand information, Reputation systems can either rely exclusively on their own observations or also consider information obtained by others.

7.4.2 Trust

The use of trust influences the decision of using second-hand information. The design choices are about how to build trust, out-of-band trust vs. building trust on experience, how to represent trust, and how to manage the influence of trust on responses.

7.4.3 Redemption and secondary response

When a node has been isolated, it can no longer be observed. The question of how those nodes should be rated over time is addressed by these two features. If the misbehavior of a node is temporary, a redemption mechanism ensures that it can come back to the network. That is, however, desirable to prevent recidivists from exploiting a redemption mechanism. This can be achieved by secondary response, meaning a quicker response to a recurring threat, in analogy to the human immune system.

7.4.4 Liar Detection

In this scenario nodes not only misbehave in forwarding (and routing), but also in the reputation system itself, by spreading spurious ratings. Untrustworthy nodes can have different strategies to publish their falsified first-hand information when attempting to influence reputation ratings (e.g., when they want to discredit regular nodes).If the lies are big, they will not pass the deviation test of CONFIDANT. A more sophisticated alternative is stealthy lies. Although nodes do not know the content of the reputation ratings held by others, they could try to infer from published first-hand information and then lie only enough to just pass the deviation test. CORE does not consider negative ratings, so only flattering has an impact. SORI are vulnerable to liars that are cooperative when forwarding. Context-aware detection copes with single liars or very small collusions by majority voting. Path-rater has no defense against liars.

7.5 IMPLEMENTATION OF REPUTATION SYSTEM

There are many algorithms are existing in different literatures for implementing reputation system in mobile ad hoc network. These have been implemented as an add-on to the DSR [Dynamic Source Routing] routing protocol. In MANET [Mobile Ad-hoc network] the nodes have to cooperate to find path between nodes [route discovery, route maintenance etc.].The successful design of a reputation system is decided by how the system is free from misbehaving nodes where misbehaviors are packet dropping, identity spoofing and packet modification.

References

1. Nguyen Tran,Combating Sybil attacks in cooperative systems, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, Sep 2012,
2. G. Kesidis, A. Tangpong, C. Griffin, "A Sybil-proof Referal System Based on Multiplicative Reputation Chains, IEEE Communication Letters, 2009.
3. Douceur, J. R. (2002) "The Sybil Attack," in *Proc. IPTPS*, Cambridge, MA.
4. Priyanka Goyal, VintiParmar and Rahul Rishi, *"MANET: Vulnerabilities, Challenges, Attacks, Application",* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
5. Mohammad Wazid,Rajesh Kumar Singh and R. H. Goudar, *"A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques "* International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.
6. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011.
7. IRSHAD ULLAH, SHOAIB UR REHMAN, Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols , School of Computing, Blekinge Institute of Technology, *June, 2010*,
8. Attacks on structured P2P overlay networks Simulating Sybil Attacks MismakuTefera, The Department of Information Technology and Media (ITM).
9. DiogoM´onica, Thwarting The Sybil Attack in Wireless Ad Hoc Networks.
10. PRITHA BAIDYA, Received Signal Strength Based Sybil Attack Detection having Fabricated Identities,
11. School of Education Technology, JADAVPUR UNIVERSITY, KOLKATA.
12. K. Gopalakrishnan&RhymendUthariaraj, in V.. 2011, "Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad-Hoc Network ", European Journal of Scientific Research ISSN 1450-216X Vol.57 No.3 pp.411-425.
13. Marti, S., Giuli, TJ., Lai, K., Baker, M., 2000. "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", *In: 6th International Conference on Mobile Computing and Networking*, pp.255-265. ACM, Boston.
14. J. Kong, X. Hong and M. Gerla, "A new set of passive routing attacks in Mobile ad hoc networks", Proc. IEEE Military Communication conference MILCOM, OCT. 2003

Author Profile

Shamikh Faraz received Master of computer application form UP Technical University, Lucknow and Master of technology degree in computer science & Engineering from Uttrakhand Technical University, Dehradun. He has 4 year teaching experience. He has authored 3 international research papers and 7 national research papers. He has attended many international and national seminars and conferences. His area of interest is database management system, discrete mathematics, data mining and graph theory.