An Assessment of Frequently Adopted Unsecure Patterns in Mobile Ad hoc Network: Requirement and Security Management Perspective

Jayraj Singh
Department of Information Technology, B. B. A. University, Raebareli Road, Lucknow

Arunesh Singh
Department of Information Technology, B. B. A. University, Raebareli Road, Lucknow

Raj Shree
Department of Information Technology, B. B. A. University, Raebareli Road, Lucknow

ABSTRACT
A mobile Ad hoc network (MANET) has played an imperative role in making very fast connection of mobile devices without including any centralize equipment. It is the simplest way to transfer files between two or more devices that can also act as routers. Now a day, the appropriate uses of this modern wireless communication are in emergency rescue situation, military scenarios, sensor networks, conferences and many others. Mobile Ad hoc Networks are adopted when wired networks are malfunctioning or broken down due to some unavoidable situation. This rapidly deployed network collaborates without using any preexisting fixed network infrastructure. Due to rapid deployment of mobile nodes or frequent change in network topology, security is the most important concern in Mobile Ad hoc Network. Due to its limited physical security, energy constrained operations and lack of centralized administration; Ad hoc Networks are more vulnerable to attacks than a wired networks or traditional networks. With the proliferation of cheaper, small, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. In this paper we are attempting to analyze the security attacks in Ad-hoc environment and focusing on various areas of security requirement, different types of active and passive attacks in Ad-hoc networks.

General Terms
Mobile Ad Hoc Network, Security, Secure Routing in MANETs.

Keywords
Security Goal, Security Attacks

1. INTRODUCTION
A mobile ad hoc network (MANET) is a self-configuring, infrastructure less, multi-hop temporal network of mobile devices connected by wireless links. Each device in a MANET is free to move in arbitrary manner in any direction result in change its links to other devices frequently. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) [1]. Therefore, Ad hoc networks' topologies are dynamic and easy to maintain. Thus, apart from the above discussion MANET has several salient characteristics such as dynamic topologies, resource constraints, limited physical security, mobility and multi hop [11]. Since, MANET is self-organizing, fast and easy deployed in non-reachable places across river, mountain or rural areas without fixed infrastructure. Therefore mobile ad hoc network is superior and favorable networks than wired one. However, in MANET there are also some disadvantages like no centralized controller, no infrastructure intrinsic mutual trust, capacity restricted medium etc.. The mobile ad hoc network, is much more vulnerable to attacks than a wired network due to its limited physical security, dynamically changing network topology, energy constrained operations and lack of centralized administration. Since, all the nodes in the network collaborate to forward the data, the wireless channel is prone to active and passive attacks by malicious nodes. These attacks include Denial of Service (DoS) attack, eavesdropping, spoofing, etc. [22]

2. SECURITY GOALS
In this section, we are going to introduce the security goals required in MANET. Further we are showing how these goals can be breakdown by different attacks.

2.1 Availability
Availability ensures to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents, despite Denial of Service (DOS) attacks [2] [4].

2.2 Confidentiality
Confidentiality is to keep certain information sent is never disclosed or unreadable to unauthorized users. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information Confidential is to encrypt the data [5],[16].

2.3 Integrity
Message being transmitted is never corrupted. a message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network [2].

2.4 Authentication
Authentication enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes. There is no central authority in MANET. Due to this, it is much more difficult to authenticate an entity [22]

2.5 Non-repudiation
The sender cannot later deny sending the information and the receiver cannot deny the reception. In public key cryptography, a node A signs the message using its private

key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message [5], [22]

2.6 Access control

Access control means to prevent unauthorized use of network services and system resources [6].

3. CHALLENGES

From the above discussion, we can safely conclude that the mobile ad hoc network is insecure by its nature. There is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside or outside the network. As a result, we can say that the mobile ad hoc network will need more robust security scheme to ensure the security of network than wired network. Several types of vulnerabilities in this network have been identified and analyzed in this section.

3.1 Lack of Secure Boundaries

There is no any secure boundary in the mobile ad hoc network. In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus freedom to join, leave and move inside the network automatically. Thus, the mobile ad hoc network does not provide secure boundary to protect the network from some potentially dangerous network accesses [8], [9].

3.2 Easy theft of nodes

There are many nodes which are expected to small in size in the network, thus they are easily compromised by outsider malicious. Thus due to this vulnerability a previously well-behaving node can unexpectedly become hostile.

3.3 Restricted power Supply

Due to mobility of nodes in the ad hoc network, nodes will reply on battery as their power supply method, Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests [6].

3.4 Lack of Centralized monitoring

Absence of centralized monitoring makes a critical problem for the detection attacks. Due to this, it is not easy to monitor the traffic in a highly and large scale manner of the MANET. It is rather common in the ad hoc network that benign failures such as transmission impairments and packet dropping.

3.5 Low and variable bandwidth

Wireless links have limited bandwidth than wires. Interference, noise and congestion effect also cause bandwidth to vary with surrounding conditions

3.6 Limited physical security

MANETs are generally more prone to physical security threats than traditional wired networks. Therefore, we need a strong solution to prevent from eavesdropping, spoofing, routing attacks and denial-of-service attacks. Presently, Existing link security techniques are often applied within wireless networks to reduce security threat.

3.7 Absence of Infrastructure

Ad hoc networks can be easily deployed without using any infrastructure, which restrict applicability of any classical solutions based on certification authorities and on line servers.

4. SECURITY ATTACKS

Mobile ad hoc network can be subject to many types of attacks. These can be categorized as Passive Attacks and Active attacks. Active attacks can further categorized into external attacks and internal attacks. Brief introduction of all attacks are as follows

4.1 Passive Attacks

In this attack, attacker only listens to the channel and snoop packets that contain secret information e.g. IP addresses, location of nodes etc., but don't disturb the operation of the network. These attacks cannot be easily identified. Passive attacks can be listed as eavesdropping, traffic analysis, and traffic monitoring

4.1.1 Eavesdropping

In this attack, the malicious node obtain some confidential information e.g. location, private key, public key or even password of the node that should be kept secret during transmission

4.1.2 Traffic Analysis

In this attack, attacker monitors packet transmission to infer important information such as a source, destination, and source-destination pair

4.1.3 Jallyfish Attack

In this attack, attacker responsible for unwanted delay of data packets for a random period of time. Attacker introduces the delay in sending packets that it receives. By doing this an attacker succeed to breakdown the performance of the network

4.2 Active Attacks

An active attack may either disturb the normal operation of a specific node or target to breakdown the operation of the whole network. An active attack tries to alter or destroy the information that is being exchanged [22]. Active attacks include wormhole, black hole, gray hole etc... The active attack however can be further classified into two classes: external attacks and internal attacks. External attacks launch outside the network. Such attacks can be prevented by using powerful encryption techniques for source authentication and firewalls. A special case of external attacks is the wormhole attacks. Internal attacks are launched by the internal Compromised nodes within the network. A single node or multiple nodes could launch an attack individually without collusion and co-ordinate collaboration. Therefore these attacks are very difficult to identify the internal attacks with this classification [10], [22].

4.2.1 Denial of service attack (DoS)

Denial of service attack prevents the normal use or management of communication facilities. Example is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance. In this, attacker doesn't corrupt data. He can disable services and replace them with their virtual services

4.2.2 Black hole

In black hole attack, black hole node acts like black hole in the universe. In this attack black hole node absorbs all the traffic towards itself and doesn't forward to other nodes [4], [17], [18]. In the Fig 1, Attacker gives response to node A before other nodes. Node A ignores all other reply when it receives attacker response & think route discovery has completed.

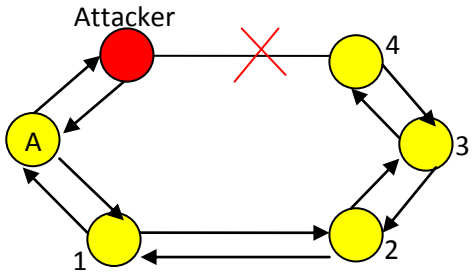

Fig 1: Black Hole Attack

There are two possible solutions for this type of attack. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. The solution of black hole attack is briefly described in [18], [27].

4.2.3 Wormhole Attack

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. The researcher Hu et al gives a concept to prevent wormhole attack [14].

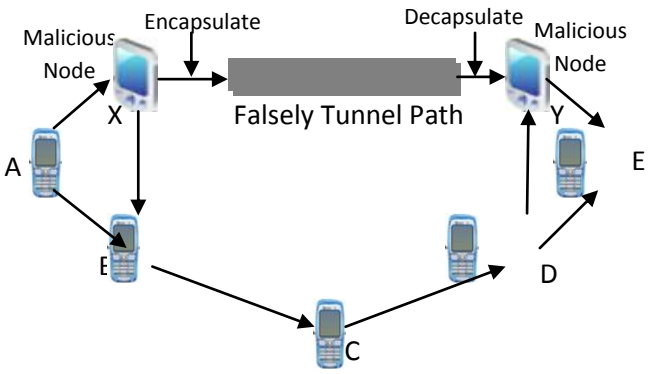

Fig 2: Warm Hole Attack

For this prevention from wormhole attack the researcher Hu et al gives a concept [14]. In his approach, each node is to compute the packet expiration time (te) based on the speed of light, and message include the expiration time (t'e) to prevent the packet from travelling further than a specific distant. At the receiving node, the packet is checked for packet expiry by comparing time and te in the message. The author also introduces TIK, which is used to authenticate the expiration time than can be modified by malicious node. In his second approach, each node must know its own position and may loosely synchronized clocks. When a source includes its current time and sending time in the packet. Therefore the receiver can judge neighbor relations by computing distant between itself and sender of packet [1].

4.2.4 Rushing attack

In this attack Rushing attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node. By this way rushing attack can slow down the performance of network. The rushing attack can act as an effective DoS attack against all currently proposed on demand MANET routing protocol [3], [5].

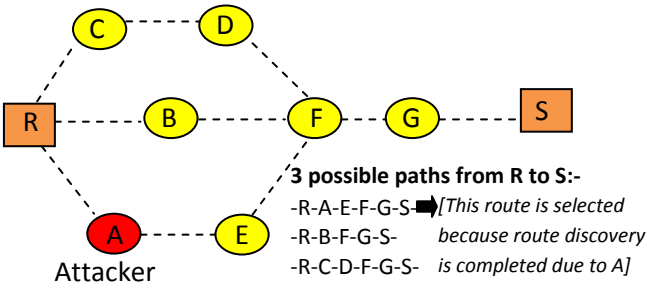

Fig 3: Rushing Attack

To protect from rushing attack, it is very necessary to detect the secure neighbor nodes. Which allows each verified neighbor is within a given transmission range. Once a node A determines that node B is a neighbor it signs a Route Delegation message, allowing node B to forward the ROUTE REQUEST. When node B determines that node A is within the allowable range, it signs an Accept Delegation message. The Randomized selection of ROUTE REQUEST message to be forwarded ensures that paths that forward REQUESTs with low latency are only slightly more likely to be selected than other paths. It also replaces traditional duplicate s on demand route discovery [1]

4.2.5 Jamming attack

In jamming attack, a malicious node initially keep monitoring of the transmission in the network and check at which frequency the communication takes place between the nodes. After that, attacker transmits the signals with the same frequency of the signal to generate weaker signals, disrupting communications, interference or noise [7].

Two types of jammer, High power pulsed full band jammers and Low power partial-band jammers, can be used. The two commonly well used techniques that overcome jamming attacks are Frequency hopping spectrum (FHSS) and direct sequence spectrum (DSSS). The author Mihui Kim and Kijoon Chae proposed a scheme to prevent this attack. In his paper they described that the whole network divided into zones and ménages the candidates' forward nodes of neighbor zones. After detecting an attack, the valid node can choose temporarily route while a main route is blocked. The valid nodes decide zones for rerouting and transmit packets for victim nodes forward nodes in the decided zones [15].

4.2.6 Sybil attack

In Sybil attack, a malicious node creates different accounts from different IP addresses in the network. Sybil attacker uses a number of nodes identities simultaneously. In this case the destination node may not be able to detect the misbehavior because the attacker may get access to all pieces of fragmented information or may alter all the packets towards the same destination [6]. Trusted certification or resource testing can be used as a solution of Sybil attack [12].

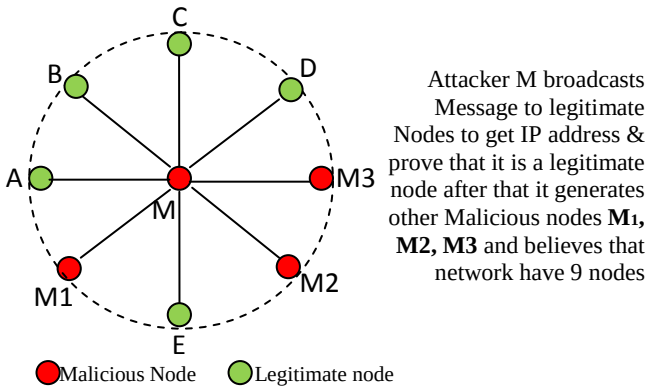

Fig 4: Sybil Attack

In trusted certification it relies on a centralized authority that must ensure each entity is assigned exactly one identity, as an indicated by possession of a certificate. And the goal of resource testing is to attempt to determine if a number of identities possess fewer resources than would be expected if they were independent. These test include checks for computing ability, storage ability, and network bandwidth, as well as limited IP addresses. [13][20]

4.2.7 Location disclosure attack

In the location disclosure attack, the attacker discloses the authentic information regarding the location or structure of the network [3].

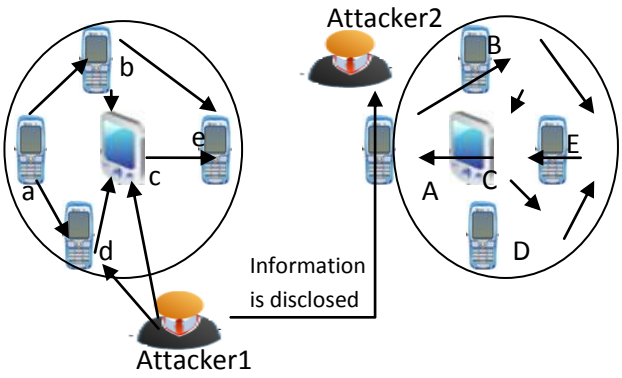

Fig 5: Location disclosure Attack

Here a malicious node which gathers the information of nodes that means route maps. And knows nodes situated on the target route through the use of traffic analysis techniques. Traffic analysis is one of the unsolved security attacks against MANETs [3]. Arjan Durresi, Vamsi Paruchuri, Mimoza Durresi, and Leonard Barolli presented a protocol [25] for achieving anonymous routing in MANET and give a concept to prevent this attack.The protocol for Anonymous Routing (PAR) guarantees absolute anonymity. PAR-Enhanced trades off some anonymity to enable detection of malicious and misbehaving nodes. A node will know the identity of any of its neighbours only if those two nodes lie on the same path of some connection. For instance, consider two neighbouring nodes A and B. A will know the identity of B only if A and B lie in the path of some connection. If no such connection exists, then A does not know B and vice versa. We assume that all the nodes are aware of some symmetric key encryption algorithm and all nodes use the same symmetric key encryption algorithm [26].

4.2.8 Byzantine attack

In this attack, a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

SMT (secure message transmission) is the secured data communication protocol against Byzantine attack [1]. For preventing this attack, A set of diverse and node disjoint paths are used at a time for data transmission and are known as Active Path Sets (APs). The whole transmission packet and the redundancy are divided into a number of pieces, and then transmit them in different ways so that from the packet pieces, the message could be reconstructed at the receiving node after transmission. By doing so, detects the faults paths using acknowledgements and threshold. And find out the byzantine links using probing signals. [21].

4.2.9 Spoofing Attack

Spoofing attack is also known as impersonation attack in which Fake messages injected into network. Spoofing attack is occurred when a malicious node misrepresents the IP and MAC address of the authentic node through which they uniquely identifies and then hide in the network. Equip nodes with GPS and calculate whether two nodes could really have a link. And node should include the 2-hop neighbors in the hello message; this gives every node a 3-hop topology of the network. But it is defeated by spoofing outside of 3-hops [8].

4.2.10 Sinkhole Attack

A sinkhole node tries to attract the data toward itself from all neighboring nodes. In this attack a malicious node generates fake routing information, and show itself as legal nodes for the route. Sinkhole node attempts to draw all network traffic according to itself, modifies the data packets, decrease the network life time, create complicated network and finally destroy the network.

4.2.11 Gray-hole attack

The gray-hole attack is also known as routing misbehavior attack. In this attack a malicious node behave as an honest node during rout discovery process. After creation of route, this malicious node silently drops packets which are sent to it. But some time node drops packets partially not only due to its malicious nature but also due to overload, congestion or Selfish nature.

4.2.12 Fabrication Attack

It is an active attack which breaks authenticity by exposed itself to become the source entity. After become a part of the network it sends error message to other legal nodes to say the route is not available any more. Thus, other node will then update their table with this false information. By this way, it drops the routing packets, forwarding packets and discloses the authentic information such as IP or MAC address of the valid nodes [26]. Watch-dogs are used to detect the fabrication attack. There are three kinds of fabrication attacks-

1) **To generate route error messages:** In this RREQ flood attack, an attacker generates many RREQ packets per unit time to an unknown IP address. As the priority of RREQ packets is greater than data packets in data flooding, the attacker first maintains the routes to destination node, then sends frequently the useless data packets, which engage the network and stop the processing of legitimate data packets.

2) **To corrupt routing information:** The other name of this attack is route cache poisoning. This kind of attack happens in DSR. In this case an attacker node advertises a zero metric for all destinations, due to this all legal nodes around the attacker node sent their packets towards it. And then the information stored in node's routing table packet is deleted, changed or injected with false information.

3) To flood routing table: If MANET is using a table-driven routing protocol, it means that the nodes try to find routing information in advance. This creates vulnerability, because the attacker will create routes to non-existent nodes. If fake routes are created too many, the false routing information will flood the routing table. In other word, real routing information will be replaced in routing tables.

4.2.13 Replay attack

This attack usually targets the freshness of routes. In this attack an attacker firstly record the message and then resend the old message to the other nodes to make update their routing table to stale routes. To add time stamp and reject the old message as suspicious and use asymmetric key to message are used for preventing replay attack

4.2.14 Resource consumption attack

In this attack, malicious node forwards unnecessary packets to the victim node and always request for route discovery to consume the battery life, network bandwidth

4.2.15 Flooding attack

In flooding attack, a malicious node may also inject false packets to consume the available resources into the network, so that valid user can not able to use the network resources for valid communication [19]. The flooding attack is possible in all most all the on demand routing protocols such as SRP, SAODV, and ARAN (Authenticated Routing for Ad-Hoc Networks) etc. flooding attack can be categorized in two categories, RREQ flooding and DATA flooding [21].

4.2.16 Route falsification attack

In a Route Falsification Attack, malicious node can work in both direction, source to destination during route request and destination to source during Route reply. When source sends request to destination node or when destination/ other node give reply for request. In this attack, malicious node falsify the route request and / or route reply packets to indicates a better/ shortest path to the source of a data connection for making large portion of the traffic go through them. When the source selects the falsified path, the malicious nodes can drop data packets they receive silently (denoted Black hole attack), on forward the packets but keep the information to conduct the analysis of communication patterns such as sender-recipient matching, traffic timing volume and shape [28].

To prevent arbitrary modification of REQ and REP packets by malicious nodes, a secure routing protocol such as Ariadne [23] requires. Secure routing information protocol (SRIP) for ad hoc networks are also designed to completely remove route falsification attack [28].

5. CONCLUSION

From the above discussion we can conclude that MANETs are more vulnerable than traditional wired networks. We discussed about almost all attacks occurred during transmission of message and their available solutions. We know that MANET is going popularity day by day due to fast & easy deployment. Now MANET has reached most of every walk of life. Therefore, a clear line of security for MANET is needed. So that people can send data securely over network.

6. REFERENCES

[1] Sudhir Agrwal, Sanjeev Jain, Sanjeev Sharma , " A survey of Routing attacks and security Measures in mobile Adhoc networks", Journal of Computing, Vol.3, Issue 1, (2011), pp.41-48 .

[2] L. Zhou, Z.J.Haas ," Securing Ad-hoc Networks", IEEE Network, (1999),pp. 24-30

[3] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei ,"A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, (2006).

[4] Hoang Lan Nguyen, Uyen Trang Nguyen "A study of different types of attacks on multicast in mobile ad hoc networks", Journal of Ad Hoc Networks, Vol.6, (2006), pp.32-46.

[5] Panagiotis Papadimitratos and Zygmunt J. Hass " Secure Routing for Mobile Ad Hoc Networks " Proceedings of the SCS Communication Networksand Distributed Systems Modeling and Simulation Conferencee, (2002), pp.1-13.

[6] Monika, Mukesh kumar, Rahul Rishi " Security Aspects in mobile ad hoc networks (MANETs)Technical Review ", International journal of Computer Applications,(2010), Journal Number 2, Article 6, pp.37-43.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhya ," Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp.265-274.

[8] Jie Yang, Yingying Chen, Trappe, W.," Detecting Spoofing Attacks in Mobile Wireless Environments", proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc communications and Networks, (2009), pp.1-9.

[9] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia hang, "Security in mobile ad hoc networks: Challenges and solutions,"IEEE Wireless Communications, Vol. 11, (2004), pp. 38-47.

[10] T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. SivaRam Murthy,"Quality Of Service Provisioning In Ad Hoc Wireless Networks: A Survey of Issues And Solutions. AdHoc Networks", Ad Hoc Networks, Vol.4, pp. 83–124.

[11] Wenjia Li and Anupam Joshi ," Security Issues in Mobile Ad hoc networks (A Survey)", The 17 th White House Papers Graduate Research In Informatics at Sussex, (2004), pp.1-23.

[12] Haifeng Yu; Kaminsky, M., Gibbons, P.B., Flaxman, A.D., "Sybil Guard: Defending against Sybil Attacks via Social Networks", IEEE/ACM Transactions on Networking, Vol.16, Issue-3, (2008), pp.576-589.

[13] Pal S, Mukhopadhyay AK, Bhattacharya P., "Defending Mechanisms Against Sybil Attack in Next Generation Mobile Ad Hoc Networks", IETE Tech Rev, (2008), Vol.25, pp.209-214.

[14] Y.C.Hu, A.Perrig, and D.Johnson,"Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, Vol.24, No.2, (2006) pp. 370-380.

[15] Earl McCune, "DSSS vs. FHSS narrowband Interference performance Issues", Magzine RF Signal Processing, (2000), pp. 90-104.

[16] W. Lou and Y. Fang, "A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions," Ad Hoc Wireless Networking, X. Chen, X. Huang, and D.-Z. Du, eds., Kluwer Publisher, Mar. 2003.

[17] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park,"Black hole attack in mobile Ad Hoc networks", In Proceedings of ACM Southeast Regional Conferenc, (2004), pp.96-97.

[18] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das,"Security Measures for Black Hole Attack in MANET:an approach", International Journal of Engineering Science and Technology, (2011), Vol.3, No.4, (2011), pp.2832-2838.

[19] Shishir K.Shandilya ,Sunita Sahu,"A Trust Based Security Scheme for RREQ Flooding attack in manet", International Journal of Computer Applications, Vol.5, No.12, (2010), pp. 0975 – 8887.

[20] Ali Ghaffari," Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, (2006), pp.124-129.

[21] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour,"A survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications,Vol.14, Issue 5, (2007), pp.85-91.

[22] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang,"Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol. 11, (2004), pp.38-47.

[23] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, " Ariadne: A secure on-demand routing protocol for ad hoc networks", Wireless Networks, Vol.11(1-2), (2005), pp.21–38,

[24] Rajendra V. Boppana Xu Su, "Secure Routing Techniques to Mitigate Insider Attacks in Wireless Ad Hoc Networks", Proceedings of IEEE Wireless Hive Networks Symposium, (2007).

[25] Arjan Durresi, Vamsi Paruchuri, Mimoza Durresi, and Leonard Barolli, "Anonymous Routing in Wireless Mobile Ad hoc networks to prevent location Disclosure Attacks", In Proceedings of EUC Workshops'2005, pp.238~247.

[26] Jeffrey Dwoskin, Dahai Xu, Jianwei Hung, Mung Chiang, Ruby Lee, "Secure Key Management Architecture Against Sensor Node Fabrication Attack", Proceedings of IEEE GLOBECOM, (2007), pp.166-171.

[27] S. Sharma, Rajshree, R.P. Pandey, V. Shukla, "Bluff-Probe Based Black Hole Node Detection and prevention", Proceedings of IEEE international Conference, IACC 2009, pp. 458-461.

[28] Rajshree, Ravi Prakash Pandey, Sanjeev Sharma, Vivek Shukla, "SRIP: A Secure Hybrid Routing Information Protocol for WSN", Chapter in Strategic Pervasive Computing Applications: Emerging Trends, (2010), pp.99-110.

[29] Raj Shree, Sanjay Kr. Dwivedi and Ravi Prakash Pandey. "Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol.18 (5), (2011), pp. 6-10.