A Survey of Attacker Malicious Maneuvering and Different Security Scheme in MANET

Rohit Chourasia[1], Abhishek Thoke[2]

[1]*MTech Research Scholar,* [2]*Research Guide*

Department of Computer Science & Engineering, TIT-Excellence, Bhopal

Abstract - The mobile nodes are independent work as intermediate node as well as sender and receiver. The connection establishment and data sending is possible through routing protocols of MANET. The routing protocols of MANET are not same as traditional wireless routing protocols. One major issue on this network is security. The perception and structure of MANET creates them flat to be easily attacked using numerous techniques often used alongside wired networks as well as new methods particular to MANETs. Security issues begin in many different fields counting with physical security, key management, routing and Intrusion Detection and prevention, many of which are vital to a functional MANET. In this paper the center of attention is on the security issues related to MANET routing protocols. The routing in MANET remains a key issue because of that without accurately functioning of routing protocols, the network cleanly will not work the technique it's intended to. Regrettably, routing also one of the most difficult to protect against attacks malicious activities because of the absence of centralized authority in MANETs. We present the main protection menace involved in routing with dynamic network as well as the recent solutions against different attacks proposed by various researchers in MANET.

Index Terms—Security, Attack, Routing, Survey, MANET, Malicious activities.

I. INTRODUCTION

The Wireless Network is the network in which the communication between the sender and receiver host is possible without any cable connection. The wireless network is advanced to wired network because it reduced the cost of extra link is connected to particular host in the network. The different devices in wireless network are performing their role efficiently to maintain the reliable connection in between source to destination. The MANET (Mobile Ad hoc Network) is the wireless network in which each and every mobile device is work as both router and host [1]. The no centralized authority is present in this network for supervision of proper communication. That's why attackers or malicious nodes are easily degrades the network performance. Each mobile device is able to communicate with each other if they are under the communication range. The nodes in range are the neighbor nodes and each node is also moves in network with random mobility speed in meters second. Due to movement of mobile nodes the string connection establishment is also the major concern for successful data delivery [2].The MANET is contemptible then other networks and also easily established at any area. The example of MANET are mentioned in figure 1, where sender node want to communicate with receiver through intermediate nodes and whole network works without any supervision authority.

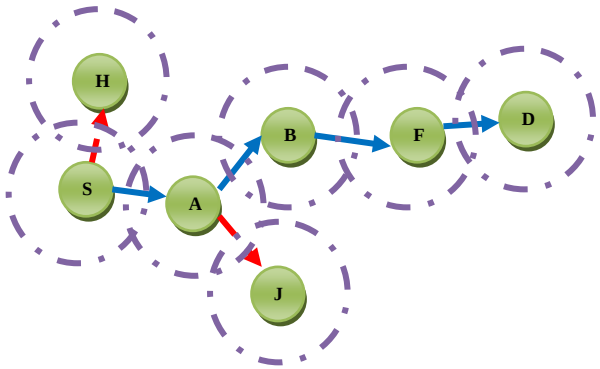

Fig.1 MANET Example

The node H and J are not further communicated with other node because they are not in range of other nodes or destination. The attackers or malicious nodes are easily disturbing the original routing performance [3]. The attacker node is always the intermediate node/s and this node/s are not instantly attack in network but these nodes are first analyze the routing information and exactly behaves like the normal node. If the sender started the data sending at that instant attacker is activated and drop or corrupt all valuable information [4]. Some of the malicious nodes are also flooding unwanted information in huge amount. The malicious nodes or attackers are of many types like blackhole attack, wormhole attack, Sybil attack and sinkhole attack. These are the packet dropping attack. The aim of that kind of attackers is to drop the useful data of sender and degrades network performance. The common thing in these MANET attackers is they all forward fake information. The blackhole attacker is communicating with destination through fake reply of original route message. The wormhole attacker is also same as established connection and at the time of data delivery all data packets dropped by attacker. The Sybil attacker is generating fake reply in the network and other network host name. The attacker are also categorized in different categories and these categories are mentioned the attacker type in network.

The attacker aim is only to drop the packets, consume network bandwidth or link capacity between the mobile nodes and communicate with fake identity in network. In this survey the different attacks classification in MANET and types of routing protocols is detail discussed with different routing strategy in MANET.

II. APPLICATION OF MANET

Mobile ad hoc network has dynamic network and fewer infrastructures so it is gaining popularity. Ad hoc networks can be established [1, 2] anywhere where the nodes have connectivity with other nodes and can join and leave the network at any time. The applications [1, 5] are as followed:

A. Military:

The communication among the soldiers, headquarters of military and vehicles can be possible as this area do not have the proper establishment of the base station for the communication.

B. Emergency Services:

This network can be used in emergency operations such as search and rescue, recovery from disasters for e.g. Fire, flood, volcano earthquake, eruption etc.

C. Commercial environments:

MANET can autonomously link an instant in business so as to share the daily updates of office. The office areas are not limited, so that this network is relay helpful for sharing information.

D. Classroom

Conducting lectures in classroom. The school teacher is conducting the online lecture or any announcement in school class rooms.

III. MAJOR CHALLENGES IN MANET

The better routing performance in network will lead to an increase in computational and communicational cost. In other words, it requires more time to setup a connection and maintains more state information per connection. The improvement in network utilization improves packets receiving, counterbalance the increase in state information and the associated complexity and various issues are needed to be faced while providing better performance for MANET. The major problems [6] that are faced are as follows:-

Unreliable channel: The bit errors are the main problem which arises because of the unreliable wireless channels. These channels cause high bit error rate and this is due to high interference, thermal noise, multipath fading effects and so on. This leads to low packet delivery ratio. Since the medium is wireless in the case of MANETs, it may also lead to leakage of information into the surroundings.

Maintenance of route: The dynamic nature of the network topology and changing behavior of the communication medium makes the maintenance of network state information very difficult. The established routing paths may be broken even during the process of data transfer. Hence the need for maintenance and reconstruction of routing paths with minimal overhead and delay causes. The QoS aware routing would require the reservation of resources at the intermediate nodes. The reservation maintenance with the changes in topology becomes cumbersome.

Mobility of the node: Since the nodes considered here are mobile nodes, that is they move independently and randomly at any direction and speed, the topology information has to be updated frequently and accordingly so as to provide routing to reach the final destination which result in again less packet delivery ratio.

Limited power supply: The mobile nodes are generally constrained by limited power supply compared to nodes in the wired networks. Providing QoS consumes more power due to overhead from the mobile nodes which may drain the node's power quickly.

Lack of centralized control: The members of any ad hoc networks can join or leave the network dynamically and the network is set up spontaneously. So there may not be any provision of centralized control on the nodes which leads to increased algorithm's overhead and complexity, as QoS state information must be disseminated efficiently.

Channel contention: Nodes in a MANET must communicate with each other on a common channel so as to provide the network topology. However, this introduces the problems of interference and channel contention. For peer-to-peer data communications these can be avoided in various ways. One way is to attempt global clock synchronization and use a TDMA-based system where each node may transmit at a predefined time. This is difficult to achieve since there is no centralized control on the nodes. Other ways are to use a different frequency band or spreading code (as in CDMA) for each transmitter. This requires a distributed channel selection mechanism as well as the dissemination of channel information.

Security: Security can be considered as a QoS attribute. Without adequate security, unauthorized accesses and usages may violate the QoS negotiations. The nature of broadcasts in wireless networks potentially results in more

security exposures. The physical medium of communication is inherently insecure. So we need to design security-aware routing algorithms for ad hoc networks.

IV. ROUTING PROTOCOLS OVERVIEW

In wireless network all the devices are connected with each other in the air or without any physical link in between source to destination. The particular destination is recognizes the source and accept their request of receiving data. The source and destination are not directly connected with each other, because of that the direct communication is possible through intermediate devices. The routing is necessary to find destination and established connection in between source to destination to deliver data. The MANET routing protocols are completely different from the traditional wireless routing protocols. In MANET the nodes are work in open environment without any supervision of any authority. The nodes are incessantly moves in area and due to that successful routing is the major issue in MANET. The routing protocols in MANET are completely different from traditional wired and wireless routing protocols [7]. The sender is finding the destination through routing procedure in network. The routing protocol is maintain the record of each route indirectly through intermediate nodes and the function of intermediate nodes are to forward the request of sender to next node till the destination is not found. The request of sender is reached to destination through number of route then the destination only select the smallest or sort route for data deliver by that the sender selects shortest path for communication to destination. In MANET there are different category of routing protocols are exist and each and every protocol has different routing procedure to establish connection in between source to destination. The routing protocols in MANET are differentiating according to different routing strategy. The classification of routing protocols on the basis of structure is mentioned in figure.2.

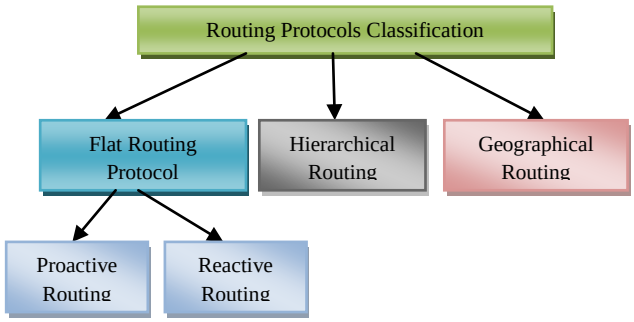

Fig.2 Classification of Routing Protocols

A. Flat Routing

The Flat network structure contains the types of routing protocols first one is Proactive or Table Driven and second in Reactive or On demand routing [7]. The actual functioning of protocol is only based on these two classifications.

1) Proactive or Table Driven Routing

Proactive protocols maintain unicast routes between all pairs of nodes regardless of whether all routes are actually used. Therefore, when the need arises, the source node has a route readily available and does not have to incur any delay for route discovery. These protocols can also find optimal routes. These protocols are broadly classified into the two traditional categories: distance vector and link state. In distance vector protocols, a node exchanges with its neighbours a vector containing the current distance information to all known destinations; the distance information propagates across the network transitively and routes are computed in a distributed manner at each node. On the other hand, in link state protocols, each node disseminates the status of each of its outgoing links throughout the network in the form of link state updates. DSDV (Destination Sequence Distance Vector) and OLSR (Optimize Link State Routing) is the example of proactive routing protocol in MANET.

2) On Demand Routing

On-demand (reactive) routing presents an interesting and significant departure from the traditional proactive approach. Main idea in on-demand routing is to find and maintain only needed routes. Recall that proactive routing protocols maintain all routes without regard to their ultimate use. The obvious advantage with discovering routes on-demand is to avoid incurring the cost of maintaining routes that are not used. This approach is attractive when the network traffic is sporadic and directed mostly toward a small subset of nodes. AODV (Ad hoc On Demand Distance Vector Routing) and DSR (Dynamic Source Routing) is the example of reactive routing protocols.

B. Hierarchical Routing

Normally, the wireless network size is increase (beyond certain thresholds), current “flat” routing schemes become not feasible because of link and processing overhead. One way to solve this problem and to produce scalable and efficient solutions is hierarchical routing [8]. An example of hierarchical routing is the Internet hierarchy, which has been practiced in wired network for a long time. Wireless hierarchical routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside of a group. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole), thus control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading

node (clusterhead) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. As mobile nodes have only a single omni-directional radio for wireless communications, this type of hierarchical organization will be referred to as ”logical hierarchy” to distinguish from the physically hierarchical network structure. The ZRP (Zone Routing Protocol) and CGSR (Cluster Gateway Source Routing Protocol) is the example of that type of routing.

C. Geographical Routing

The Geographical routing protocols [9] imply that the hosts participating in the routing process should be aware of their geographic positions. An advantage of geographic routing protocols is that they prevent network-wide searches for destinations. Control and data packets can be sent in the general direction of the destination if the recent geographical coordinates are known. This reduces control overhead in the network. A disadvantage is that all nodes must have access to their geographical coordinates all the time to make the geographical routing protocols useful. The routing update must be done faster than the network mobility rate to make the location-based routing effective. This is because the nodes locations may change quickly in a mobile ad hoc network. There are two approaches to geographic mobile ad hoc networks

1. Actual geographic coordinates (as obtained through GPS-the Global Positioning System).
2. Reference points in some fixed coordinate system.

The example of Geographical Routing Protocol is DREAM (Distance Routing Effect Algorithm for Mobility) and LAR (Location Aware Routing).

D. Problems in MANET Routing

There are many types of routing protocols in MANET but the strong link due to dynamic topology is not established. Following are the problems with routing in [10] MANET are as follows:-:

1) Asymmetric links

The links in MANET are asymmetric because of the mobile nature of nodes and their continuously changing position within network. But wired networks are always fixed therefore can rely on the symmetric links.

2) Routing Overhead

As nodes are mobile, their positions are continuously changes therefore, in routing table some fake path/routes are generated in which leads to routing overhead.

3) Interference

This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

4) Dynamic Topology

Topology of a network can’t be constant. The nature of the mobile nodes is unpredictable, they might move or stable or characteristics of communication media might change.

V. TYPES OF ATTACK IN MANET

Attackers or Malicious nodes are performing different types of malicious activities that have damage basic aspects of security like integrity, confidentiality and privacy [11]. Here there are different types of attacks [12, 13] and their mentioned in detail.

A. Active Attacks

It is like as passive attack that monitors and listens by unauthorized communication channel and it also modifies data stream in communication channel. There are different types of active attacks a shown here.

1) Blackhole Attack

Blackhole attack [14] is the packet consumption attack. In this attack the attacker nodes is identified the sender that want to send data to receiver and reply fake route information to sender. Sender sends the data from the path where the attacker is exist in network. Then in that case the attacker loss whole data and network performance degrades.

2) Sybil Attack

Malicious node can duplicate itself and it presence affects at multiple places. It targets fault tolerance scheme as distributed storage, multipath identities for another node, multipath routing and topology in the networks.

3) HELLO Flood Attack

An attacker with high radio transmission range process on power and sends “HELLO” packets to number of sensor nodes which are isolated in Mobile Ad hoc Network. So sensor nodes prejudice adversary is their neighbour. While information is sent to the base station, then at that time, the

victim nodes are trying to go via attacker resulting neighbour in higher spoofed.

4) Denial of Service

When unintentional failure of nodes or malicious nodes attack any event that diminishes network's capability of services and also affect on destroying network, this can be affected on different layers like Physical layer and DoS attacker in jamming and tampering. While collision, unfairness and exhaustion will occur in Link Layer collision.

5) Wormhole attack

Wormhole attack is most severe attack in MANET in which using private high speed networking, pair of colluding attackers can record packet information at one location and replay then on other location. So this can be launched against all communications for providing authenticity and confidentiality.

B. Passive Attacks

It does not affect any communication works but unauthorized person can just monitor and listen communication channel and it is hard to find these types of attacks due to its passiveness behaviour.

1) Attacks against privacy

In MANET there are large numbers of information available by remote access, so any malicious node can easily gather information. Here some other attacks which come in category of passive attack are defined.

2) Monitor and Eavesdropping

It is very common attack, in which, by snooping data adversary it can easily discover communication control information for mobile network configuration that contains information and affects against privacy protection.

3) Traffic Analysis

Though messages are transferred by encrypted, it leaves high possibility communication patterns, because of sensor activities and it can potentially affect on enable information and cause harm to dynamic network.

VI. LITERATURE SURVEY

In this section we actually discuss the work in field of security is proposed by different researchers. Many researches are interested to provide security in network.

Sumaiya Vhora, Rajan Patel, Nimisha Patel in this paper, [15] proposed the scheme that detect the packet drop attack and provide the trusted paths. Using RBDR record base scheme, the accurate analytical view of network behavior can detect and prevent packet drop attack at network layer for MANET. The RBDR scheme is used to view and analyze of network behavior for detecting and preventing packet drop attack at network layer for MANET. The proposed method can not only identify the abnormal route, but also acknowledge the whole network about this route with the possibility of malicious node to prevent future routing.

Tao Shu and Marwan Krunz in this paper [16] assumed that source and destination are truthful in following the established protocol because delivering packets end-to-end is in their interest. Misbehaving source and destination will be pursued in their future research. Moreover, in this paper, as a proof of concept, they were mainly focused on showing the feasibility of the proposed cypto-primitives and how second order statistics of packet loss can be utilized to improve detection accuracy. This work targets the challenging situation where link errors and malicious dropping lead to comparable packet loss rates. In particular, They are interested in the problem of detecting the occurrence of selective packet drops and identifying the malicious node(s) responsible for these drops.

Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes Penalver in this paper [17], proposed the design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. Moreover, they presented a mechanism to allow nodes to check the authenticity of their IP addresses while not generating duplicated IP addresses. The mechanism helps nodes to authenticate by using their IP addresses. They have used this mechanism in the secure protocol presented in this paper, but it can be replaced by any other IP address assignment mechanism.

Swagata Singha, Abhijit Das in paper [18] proposed the scheme that has work in two phases. The first criterion that has been checked is the authenticity of a new node that wants to join the network. For this they proposed a secure algorithm based on cryptography. After authenticating it, if the node is approved to be reliable, then it is authorized to some of the network related jobs. In spite of granting full authorization, they move on to the second phase of detection if the newly joined node is found to be malicious. For this, they send an entire data set divided into some smaller parts. The node is able to construct an entire data getting minimum number of those data parts if it is non-malicious. If not, the same process is repeated again with an increase in the minimum number data sets to construct the

original data. Post this phase; in case the node is detected to be malicious, then it is eliminated from the network. Otherwise it is allowed to join the network as a completely trusted node.

S Remya, K S Lakshmi in this paper [19] proposed a Secured Hierarchical Anonymous Routing Protocol for MANETs. SHARP is cluster or group based anonymous routing protocol. Here the nodes in the network are grouped. The grouping is based on range and position of each node. The node and its one hop neighbours are grouped together. That means the nodes with a particular distance are grouped together to form a cluster SHARP provides source, destination and route anonymity. Encryption based inter group routing is established in SHARP. Research has to be continued to make encryption based routing to extend the anonymity of SHARP. The anonymity can be enhanced by encrypting the intra group communication. To improve the security, encryption by other methods better than RSA will also be considered.

Wei Liu, Ming Yu In this paper [20], focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. They assume there is no online security or localization service available when the network is deployed. They propose an authenticated anonymous secure routing (AASR) to overcome the aforementioned problems. They adopt a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ–RREP linkage. The group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet. Extensive simulations are used to compare the performance of AASR (Authenticated Anonymous Secure Routing) with that of ANODR (ANonymous on demand routing), which is a representative on-demand anonymous routing protocol.

Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu in this paper [21], proposed the solution of problem of selfish replica allocation. Simply, selfish replica allocation refers to a node's non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes. In this proposed scheme a selfish node detection method and novel replica allocation techniques is handle the selfish replica allocation appropriately. The proposed strategies are inspired by the real-world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own discretion. They applied the notion of credit risk from economics to detect selfish nodes. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness.

Rajendra V. Boppana, and Xu Su in this paper [22], proposed scheme enumerate false positives and analyze their impact on the accuracy of monitoring-based intrusion detection. They use a combination of experimental, analytical, and simulation analyses for this purpose. First, using a linear chain of three off-the-shelf wireless routers, it show that a sender of data packets falsely suspects, based on the monitoring of transmission activities in its radio range, its next hop of not forwarding its packets. In the unlikely event of an attack, the detection will take a long time since malicious nodes can exploit the detection rule by alternating between normal and attack modes and stay undetected for long periods.

VII. CONCLUSION

The Mobile Ad hoc networks are open network and by that the attackers are easily bespoke and drop the valuable information of sender. The network is completely dynamic by that the attacker confirmation and capturing is the difficult task. The different security techniques like encryption decryption and Intrusion Detection System are proposed by different authors to secure communication in between sender to receiver at different layers of network and also prove that the various kinds of susceptible attacks are harmful for dynamic, wireless and infrastructure less network. The routing protocols in MANET are fairly anxious because attackers or malicious nodes can easily acquire information about network topology at the time of route establishment. Indeed in MANET routing protocols, the route finding packets are agreed in clear text. So a malicious node affect original routing performance by learning the network composition just by examine type of packets (data packet or connection packet) and may be able to determine the role of each node in the network. Through all these information a malicious node attacks performed in order to perturb the original network operation by isolate actual important nodes, etc. That is the achievement of instantaneous network despite of the types of nodes or type of environments that is customary which is express in this paper. The different author work are very effective and unique and this work is also provides the thoughts to other researchers that are try to do something new in field of security in MANET.

VIII. EXPECTED OUTCOME

After reading various researcher work discussed in this papers in field of security in MANET, we motivated to work on packet dropping attack in MANET. One of the simplest way for an attacker node to perturb the good function of MANET is to announce better routes (to reach to other neighbor nodes or just a specific one) than the other nodes. In addition all these vulnerabilities there are the existence of security routing protocols which make them secure and attacker infection free networks there by

admiring the ultimate aim of researcher in field of Mobile Ad hoc networks. I proposed the variable consistency based security scheme to identify the attacker on the basis of actual route selection. If the actual route is identified by Intrusion Detection System (IDS) it also identified the attacker and also prevent network from the attacker. The proposed method will improve network routing performance measure through performance metrics like throughput, packet dropping and routing load in presence of attacker after applying proposed security scheme.

REFERENCES

[1] C Siva Rama Murthy C. and B.S Manoj, “Ad Hoc Wireless Networks, Architectures and Protocols”, Second Edition, Low price Edition, Pearson Education, 2007.

[2] Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle, " A Survey of Survivability in Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, First Quarter 2009

[3] Y. Khamayesh,R.Salah and M.B. Yassein. “Malicious Nodes Detection in MANETs: Behavioral Analysis Approach”, Journal of Networks, Vol.7, No.1, January 2012.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Proceedings of MobiCom 2000, August 2000.

[5] G. S. Mamatha1 and Dr. S. C. Sharma Analyzing The MANET Variations, Challenges, Capacity And Protocol Issues International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[6] Sanjeev Gangwar, Dr. Saurabh Pal and Dr. Krishan Kumar, "Mobile Ad Hoc Networks: A Comparative Study of QoS Routing Protocols", IJCSET Vol 2, Issue 1, pp.771-775, January 2012.

[7] Elizabethm . Royer, Chai-Keong Toh, "A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April 1999.

[8] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002

[9] Fraser Cadger, Kevin Curran, Jose Santos, and Sandra Moffett", A Survey of Geographical Routing in Wireless Ad-Hoc Networks, IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013.

[10] B.N. Jagdale, Pragati Patil, P. Lahane, D. Javale, "Analysis and Comparison of Distance Vector, DSDV and AODV Protocol of MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012.

[11] Congzhe Zhang, MengChu Zhou and Ming Yu, " Ad hoc network routing and security: A review", International Journal of Communication Systems (IJCS), published in Wiley Science, pp. 909–925, 2007

[12] Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE 15th International Conference on Computer Modelling and Simulation, 2013.

[13] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-407, 2010.

[14] Swati Jain, Naveen Hemrajani, “Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview”, International Journal of Science and Research (IJSR), India Online ISSN: 2319- 7064, Volume 2 Issue 5, May 2013.

[15] Sumaiya Vhora, Rajan Patel, Nimisha Patel, " Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015.

[16] Tao Shu and Marwan Krunz, “Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, IEEE Transactions On Mobile Computing, Vol. 14, No. 4, April 2015.

[17] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes, “A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”, IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 4, April 2013.

[18] Swagata Singha, Abhijit Das, “Detection and Elimination of the Topological Threats in Mobile Ad Hoc Network: A New Approach”, IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015

[19] S Remya, K S Lakshmi, “SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs”, IEEE International Conference on Computer Communication and Informatics (ICCCI-2015), Jan. 08 – 10, 2015, Coimbatore, INDIA.

[20] Wei Liu, Ming Yu, “AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments”, IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, November, 2014.

[21] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, “Allocation Over a Mobile Ad Hoc Network Handling Selfishness in Replica”, IEEE Transaction On Mobile Computing, Vol. 11, No. 2, February 2012.

[22] Rajendra V. Boppana, and Xu Su, "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 10, No. 8, August 2011.