International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 08, August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A REVIEW PAPER ON SECURITY IN MOBILE ADHOC NETWORK

Anuj Mehta[1], Ravina Saini[2]

[1,2] *CSE, SKIET KUK , (India)*

ABSTRACT

Mobile Ad hoc network (MANET) is a collection of self configuring, multi-hop wireless network. Due to the mobility and dynamic nature of MANET, network is not secure. MANET is more vulnerable to different types of attacks and security threats because of its characteristics. A routing protocol in a mobile Ad hoc network should be against both inside and outside attackers. Most of the routing protocols in MANETs assume that all the nodes in a network will cooperate to each other while forwarding data packets to other nodes. But intermediate nodes may cause several problems like it can deny to forward the packet, can also extract useful information from the packet or may modify the content of packet. Such nodes are referred as malicious nodes. We present a survey of the main types of routing protocols and some security threats and various detection secheme against attack.. This paper also classifies several common attacks against the ad hoc networks routing protocols based upon the techniques that could be used by attackers to exploit routing messages.

Keywords: MANET, Attack, Detection Seheme , Routing Protocol

I. INTRODUCTION

Mobile Adhoc network is a gathering of self configuring , multihop wireless network that can change location and configure itself on the fly. Because MANET are Mobile , they use wireless connection to communication to various network .Due to mobility and dynamic nature of MANET , it is not secure. There are many routing protocol in MANET assume that all the nodes in network will cooperate to each other while forwarding data packets to other nodes .But intermediate nodes can create the problem several problem in the network like it can deny the forward packet , can also get useful information from the packet or can modify the content of packets..such nodes are reffered as malicious nodes

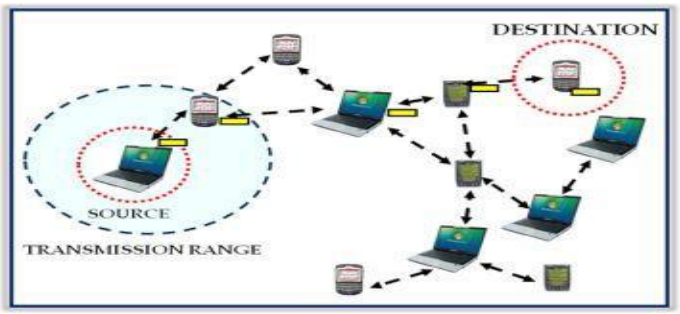

Fig 1.1 Data Transmission in MANET

II. LITERATURE SURVEY

In this paper [1], authors try to solve the issues of black hole and gray hole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS).

It merge the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio.

It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in MANET for the gray hole and black hole attacks.

Cooperative Bait Detection Scheme (CBDS) has been used to tackle black hole and gray hole attacks caused by malicious nodes [1]. CBDS combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique.

In this paper [2], authors proposed self organized algorithm. Self organizing algorithms are responsible for no. of solutions to the management of MANETs. Best nodes are chosen to act as leaders and the tasks are being assigned to them. Selfish nodes misbehave in order to avoid from being selected as leader as they are not interested in serving other nodes. Malicious nodes once selected as leader then launches, the Denial of Service (DoS) attack which may lead to problems in network functioning. In self-organizing mechanism the nodes participating cooperates with each other in detecting the malicious leader. The mechanism declares the malicious behaving leader while protecting normal behaving to be declared as malicious one. The mechanism is applicable to every leader based network and is even applicable to & effective for large MANETs.

In this paper [3], authors explained that Game theoretic approach is used. Game theoretic approach is very useful in addressing problems where multiplayer's with contradictory goals complete with each other. This theory provides powerful mathematical tool for problems with multiplayers. Most of works applies game security model considering two players- an attacker side and a defender side. In multiplayer's all the defenders are treated as one player and all the attackers are treated as another player In Game theory mechanism each node needs to know only its own state information and aggregate effect of the other nodes in the MANET network. It's a fully distributed scheme. In future the mechanism could be extended to multiple attackers and multiple defenders.

In this paper [21], authors discussed about MANET. With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results the rapid development of the technology. Due to MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention. The common routing protocols in current such as DSR AODV and so on almost take account in performance.

They don't have the related mechanism about detection and response. Aiming at the possible attacks by malicious nodes, based on the DSR protocol, this paper presented a mechanism to detect malicious nodes launching black/gray-hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks.

III. ATTACK ON MANET

At the highest level, the security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. *Authentication* isthe verification of claims about the identity of a source of information. *Confidentiality* means that only authorized people or systems can read or execute protected data or programs.

3.1 Passive Attacks

In a uninvolved assault an unapproved hub screens and means to figure out data about the system. The assailants don't generally need to correspond with the system. Subsequently they don't disturb interchanges or bring on any immediate harm to the system. In any case, they can be utilized to get data for future unsafe assaults. Cases of aloof assaults are listening in and activity investigation.

3.1.1 Eavesdropping Attacks: also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyse broadcast messages to reveal some useful information about the network.

3.1.2 Traffic Analysis: is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;
- the current sources and destination of communications; and

3.2 Active Attacks: These attacks cause unauthorised state changes in the network such as denial ofservice, modification of packets, and the like. These attacks are generally launched by users or nodes with authorisation to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

3.2.1Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes,if the dropping node is at a critical point.

3.2.2 Modification Attacks: In sider attackers modify packets to disrupt the network. For example, in the **sinkhole attack** the attacker tries to attract nearly all traffic from a particular area through a compromised node by making the compromised node attractive to other nodes.

A black hole attack is like a sinkhole attack that attracts traffic through itself and uses it as the basis for further attacks. The goal is to prevent packets being forwarded to the destination. If the black hole is a virtual node or a node outside the network, it is hard to detect.

3.3 Denial of Service (DOS) attack: A DoS attack [9] may be defined as an event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. DoS attack may temporarily block service availability or permanently distort information in the network. DoS attacks can exhaust limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. Networks are attacked by modifying routing information or changing system configuration, thereby directly attacking data integrity.

Fig 1.7 DOS Attack

IV. DETECTION AND PREVENTION SCHEME AGAINST ATTACK

4.1 Techniques for Detection and Prevention of Gray Hole

4.1.1 Wormhole Detection Techniques

4.1.1.1 Distance and location Based: Packet Leash Technique.

Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash (Yih-Chun Hu et.al, 2003) is the method that defends against the wormhole attack. The leashes can be grouped either into geographical or temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and secure synchronized clock. Whenever a sender sends the data packet, it includes its own recent location and transmission time in header. Therefore, the receiver is capable of predicting the neighbour relation by calculating the distance between itself and source. In temporal leashes, all nodes calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack.

Geographical leashes are more advantageous than temporal leashes as they do not require a tightly synchronized clock. It has the limitations of GPS technology.

4.1.2 Wormhole Prevention Techniques

4.1.2.1 Path Tracing Approach

There are two phases in Path tracing approach as described below.

Phase I

The source node floods the route request (RREQ) packets through immediate neighbours towards destination. When it reaches the destination, it sends back route reply (RREP) in the reverse path.

The path details are stored in the DSR routing cache. In order to detect the wormhole, we optimize the general DSR header by adding extra fields. Prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet.

We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. All nodes that participate in the routing mechanism perform this operation.

Phase II

1 Each node in the network has to perform four major operations to detect the wormhole attack. Compute per hop distance and compare it with the prior per hop distance.

2. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value.

3. If it is larger, then the wormhole is detected and it is informed to all other nodes in the networks to provide wormhole alertness.

4.For the confirmation of wormhole attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.

5. If DBC - DAB > RTh and FAcount > FATh then it is a wormhole link.

4.2 Techniques for Detection and Prevention of Gray Hole

Gray Hole Attack :Several techniques have been proposed for detection and prevention of gray hole attack in MANET. H. Fu et albproposed an algorithm in which an additional Data Routing Information (DRI) table is maintained by each node. In the DRI table, 'true' is represented by 1 and 'false' is represented by 0.The first bit "From" denotes that the node has routed data packets from the node while the second bit "Through" denotes that the node has routed data packet through the node (in the Node field).

When any nodeB received data packet from one of its neighbours or any node that sent data packets through one of its neighbours, the DRI entry is updated automatically. It is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attack. This is the main drawback of this algorithm. It takes O (n2) time whenever a node decides to send packets to another node. Nodes in ad hoc networks move randomly, a true node which has recently moved in the vicinity of a node may be treated as black hole as it might not have done any data transfer through or from the other neighbouring nodes. Hence the updating of DRI entry must also take into account the mobility of nodes. A. M. Kanthe et al proposed an algorithm to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates and checks the peak value whether reply packet sequence number is less than or not.

The parameters used to calculate the peak value are: a) Routing table sequence number. b) Reply packet sequence number. c) Elapsed time of ad hoc network which is analogous to current simulation time of simulator

in simulation environment. d) Total number of reply packets received by the intermediate/neighbour/replying node. e) Reply Forward Ratio (RFR) of replying node.

4.3 Techniques for Detection and Prevention of Black Hole

Black-Hole Attack: (I) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found. (ii) Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

V. ROUTING PROTOCOL

5.1 Proactive Routing

Proactive protocols rely upon maintaining routing tables ofknown destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using known routes, however routing tables must be kept up-to-date; this uses memory and nodes periodically send update messages to neighbours, even when no traffic is present, wasting bandwidth **.** Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads.

- Destination Sequenced Distance Vector routing
- Wireless Routing Protocol (WRP)
- Cluster Gateway Switch Routing protocol (CGSR)
- Fisheye State Routing (FSR)
- The logical Hypercube-based Virtual Dynamic
- Backbone protocol (HVDB)

5.1.1 Destination Sequenced Distance Vector routing (DSDV*):*DSDV (Perkins & Bhagwat, 1994) is a distance vector routing protocol that ensures a loop-free routing by tagging each route table entry with a sequence number and is based upon the Bellman-Ford algorithm to calculate the shortest number of hops to the destination

5.1.2 Wireless Routing Protocol (WRP): WRP (Murthy & Garcia-Luna-Aceves, 1995) is a vector routing protocol that aims to reduce the possibility of forming temporary routing loops in mobile ad-hoc networks. It is a proactive, destination-based protocol. WRP belongs to the class of path finding algorithms. The typical feature for these algorithms is that they utilize information about distance and second-to-last hop (predecessor) along the path to each destination. Pathfinding algorithms eliminate the counting-to-infinity problem of distributed Bellman- Ford-algorithms by using that predecessor information, which can be used to infer an implicit path to a destination and thus detect routing loops.

- **Distance table,**
- **Routing table,**
- **Link- cost table and**

- **Message Retransmission List (MRL) table.**

In WRP nodes learn of the existence of their neighbors form the receipt of acknowledgements and other messages. If there are no such messages to be sent, a node must send a HELLO message within a specified time period to ensure connectivity.

5.1.3 Clusterhead Gateway Switch Routing protocol (CGSR): CGSR (Chiang, Wu, Liu, & Gerla, 1997) is a typical cluster based hierarchical routing. A stable clustering algorithm Least Clusterhead Change (LCC) is used to partition the whole network into clusters and a Clusterhead is elected in each cluster. A mobile node that belongs to two or more clusters is a gateway connecting the clusters. The major advantage of CGSR is that it can greatlyreduce the routing table size comparing to DV protocols. Only one entry is needed for all nodes in the same cluster. Thus the broadcast packet size of the routing table is reduced. These features make a DV routing scale to large network size.. The drawback of CGSR is the difficulty to maintain the cluster structure in a mobile environment. The LCC clustering algorithm introduces additional overhead and complexity in the formation and maintenance of clusters .

5.1.4 Fisheye State Routing (FSR):FSR (Pei, Gerla & Chen, 2000) is an improvement of GSR. GSR requires the entire topology table to be exchanged among neighbors. The Fisheye State Routing (FSR) is a proactive unicast routing protocol based on Link State routing algorithm with effectively reduced overhead to maintain network topology information. As indicated in its name, FSR utilizes a function similar to a fish eye. The eyes of fishes catch the pixels near the focal with high detail, and the detail decreases as the distance from the focal point increases. Similar to fish eyes, FSR maintains the accurate distance and path quality information about the immediate neighboring nodes, and progressively reduces detail as the distance increases. In FSR, however, nodes exchange link state information only with the neighboring nodes to maintain up-to-date topology information. Link state updates are exchanged periodically in FSR, and each node keeps a full topology map of the network.

5.1.5 The logical Hypercube-based Virtual Dynamic Backbone protocol (HVDB): logical Hypercube-based Virtual Dynamic Backbone (HVDB) is a proactive, QoS-aware and hybrid multicast routing protocol for large scale MANETs. It includes proactive logical route maintenance, summary based membership update and logical location-based multicast routing. Due to the regularity and symmetry properties of hypercube, no leader is needed in a logical

hypercube, and every node plays almost the same role except for the slightly different roles of border cluster heads and inner cluster heads. Thus, no single node is more loaded than any other nodes, and no problem of bottlenecks exists, which is likely to occur in tree-based architectures.

5.2 Reactive Routing Protocols

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route.

Rapidly changing wireless network topology may break active route and cause subsequent route search. References gives a very good explanation on this topic. Routes in reactive algorithms are established when they are needed, in order to minimize the communication overhead.

Some of the existing proactive/table driven routing protocols are:

- Ad-hoc On-demand Distance Vector routing

(AODV)

- Dynamic Source Routing (DSR)
- Light-weight Mobile Routing (LMR)
- Associativity Based Routing (ABR)
- The Enhanced On Demand Multicast Routing Protocol (EODMRP)

5.2.1 Ad-hoc On-demand Distance Vector routing (AODV): The Ad-hoc On-demand Distance Vector (AODV) routing is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. AODV utilizes sequence numbers and routing beacons from DSDV but performs route discovery using on-demand route requests (RREQ); the same process as the DSR protocol. AODV is different to DSR in that it uses distance vector routing; this requires every node in the route to maintain a temporary routing table for the duration of the communication. AODV has improved upon the DSR route request process using an expanding ring search mechanism based upon incrementing time-to-live (TTL) to prevent excessive RREQ flooding.

5.2.2 Dynamic source Routing: DSR allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. In this protocol, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known for a particular entry in the route cache. Routing in DSR is done using two phases: route discovery and route maintenance. When a source node wants to send a packet to a destination, it first consults its route cache to determine whether it already knows about any route to the destination or not. If already there is an entry for that destination, the source uses that to send the packet. If not, it initiates a route request broadcast. This request includes the destination address, source address, and a unique identification number. Each intermediate node checks whether it knows about the destination or not. The intermediate node does not know about the destination, it again forwards the packet and eventually this reaches the destination.

5.2.3 Light-weight Mobile Routing (LMR) The LMR protocol is based on the concept of link reversal algorithm. LMR addresses the issue of partitioned network by providing a link erasure mechanism. LMR requires two passes to re-establish and converge to an alternate route, if one exists. LMR can erase invalid routes and detect partition in a single pass. It is designed to reduce the control message propagation in highly dynamic mobile networking environment. Due to this shortest hop paths are given only secondary importance and this protocol fits under the stability criteria. The benefit of this protocol is that routes will be found rather quickly and broken links will have only local affect. It has good performance if the network connectivity is high, i.e., in the case of dense network. Routes may be redundant.

5.2.4 Associativity Based Routing (ABR):ABR protocol defines a new type of routing metric,degree of association stability for mobile ad hoc networks.In this routing protocol, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased.

A high value of associativity tick for any particular beaconing node means that the node is relatively static. Associativity tick is reset when any neighboring node moves out of the neighborhood of any other node.

5.3 Hybrid Routing Protocols

Hybrid routing protocols are a new generation of protocols, where both proactive and reactive in nature.These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. This is mostly achieved by proactively maintaining routes to nearby nodes and determining the route to faraway nodes using a route discovery strategy.

Some of the existing hybrid routing protocols are:

Temporally Ordered Routing Algorithm (TORA)

- Zone Routing Protocol (ZRP)
- Zone-based Hierarchical Link State (ZHLS)
- Sharp Hybrid Adaptive Routing Protocol
- (SHARP)
- Optimized Polymorphic Hybrid Multicast Routing
- Protocol (OPHMR)

5.3.1 Temporally Ordered Routing Algorithm (TORA) Temporally Ordered Routing Algorithm (TORA) is a reactive routing algorithm based on the concept of link reversal. TORA improves the partial link reversal method by detecting partitions and stopping non-productive link reversals. TORA is a distributed highly adaptive routing protocol designed to operate in a dynamic multihop network. TORA uses an arbitrary height parameter to determine the direction of link between any two nodes for a given destination. Consequently, multiple routes often exist for a given destination but none of them are necessarily the shortest route.

To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination.

5.3.2 Zone Routing Protocol (ZRP)*:*ZRP (Haas, 1997; Haas & Pearlman, 1998) utilizes both proactive and reactive routing strategies in order to gain benefits from the advantages of both types. It is a hybrid routing protocol which combines the advantages of both proactive and reactive approaches. It takes advantage of proactive protocol to find node's local neighborhood as well as reactive protocol for routing between these neighborhoods

5.3.3. Zone-based Hierarchical Link State (ZHLS*) :*The Zone-based Hierarchical Link State routing (ZHLS) is a hybrid routing protocol. In ZHLS, mobile nodes are assumed to know their physical locations with assistance from a locating system like GPS. The network is divided into non-overlapping zones based on geographical information. In ZHLS protocol, the network is divided into non overlapping zones as in cellular networks. Each node knows the node connectivity within its own zone and the zone connectivity information of the entire network. The link state routing is performed by employing two levels: node level and global zone level. ZHLS does not have any cluster head in the network like other hierarchical routing protocols.

5.3.4. Sharp Hybrid Adaptive Routing Protocol (SHARP): SHARP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. This protocol defines the proactive zones around some nodes. The number of nodes in a particular proactive zone is determined by the node-specific zone radius. All nodes within the zone radius of a particular node become the member of that

particular proactive zone for that node. If for a given destination a node is not present within a particular proactive zone, reactive routing mechanism (query-reply) is used to establish the route to that node.

5.3.5 The Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR): The Optimized Polymorphic Hybrid Multicast Routing protocol (OPHMR) is a proactive, polymorphic energy efficient and hybrid multicast routing protocol. It attempts to benefit from the high efficiency of proactive behavior and the limited network traffic overhead of the reactive behavior, while being power, mobility, and vicinity-density aware.

VI. CONCLUSION

A Mobile Ad-hoc Network (MANET) contains selfconfiguring, and self-operating nodes, each of them communicates with other nodes directly, without any help of centralized administration or fixed infrastructure, within transmission range of nodes .we have stuied in different types of attacks and detection and prevention techniques against the attack .We have tried to categorize the different types of routing protocol which used in transfer the data

REFERENCES

[1] Chin-Feng Lai, Han-Chieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, Member,"Defending Against Collaborative Attacks by Malicious Nodes in MANETs:A Cooperative Bait Detection Approach", IEEE, DOI:10.1109/JSYST.2013.2296197,ISSN:1932-8184, Volume:9, Issue:1,Page(s):65- 75,March 2015

[2] BabakHosseinKhala, HamidrezaBagheri, Marcos Katz, Mohammad JavadSalehi, Mohammad Noor mohammadpour, and Seyed Mohammad AsghariPari. "A Self- Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks", Wireless Days (WD), 2013 IFIP, Valencia,DOI: 10.1109/WD.2013.6686475, ISSN:2156-9711, Page(s):1 – 3, 13-15 Nov. 2013

[3] Richard Yu, Helen Tang, Minyi Huang and Yanwei Wang, *Member,"* A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks",Wireless Communications, IEEE ,ISSN:1536-1276, Volume:13, Issue:3, Page(s):1616-1627, January 2014

[4] Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India),Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India),Rashid Sheikh,"Security Issues in MANET: A Review", Wireless And Optical Communications Networks (WOCN), Colombo,DOI: 10.1109/WOCN.2010.5587317, Page(s):1 – 4,sept. 2010.

[5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China," Research on MANET Security Architecture design", Signal Acquisition and Processing,Bangalore, DOI: 10.1109/ICSAP.2010.19, Page(s):90-93, Feb 2013.

[6] Luis Javier García Villalba , Julián García Matesanz , Ana Lucila Sandoval Orozco and José Duván Márquez Díaz,"Auto-Configuration Protocols in Mobile Ad Hoc Networks",Sensors , DOI: 10.3390/s110403652,11(4), Page(s):3652-3666,25 March 2011.

[7] Nikhil R Joshi,Chandrappa D.N,"Manet Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity"

[8] Nidhi Saxena,Vipul Saxena, Neelesh Dubey, Pragya Mishra,"REVIEW PAPER ATTACK ANALYSIS IN MOBILE AD HOC NETWORK BASED ON SYSTEM OBSERVATIONS", IJARCSSE, ISSN:2277-128X,Volume:3, Issue:7, Page(s):618-623, July 2013.

[9] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria,"Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", Australian Journal of Basic and Applied Sciences, ISSN 1991-8178, Volume:5,Issue:10,Page(s): 1137-1145,2011

[10] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of Blackhole Attack in MANET Using ACO", International Journal of Computer Science and Network Security, Volume:12, Issue :5, Page(s):21-24, May 2012 .

[11] Usha,Bose," Understanding Black Hole Attack in Manet", European Journal of Scientific Research, ISSN: 1450-216X, Volume:83,Issue:3, Page(s):383-396, 2012.

[12] Mansoor Alicherry, Angelos D. Keromytis, "Securing MANET Multicast Using DIPLOMA", Adavances in computers and information security, ISSN: 0302-9743, Volume 6434, Page(s):232-250, 2010.

[13] K. Biswas anormatid Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March2007.

[14] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[15] Mieso K.Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", SYSTEMICS, CYBERNETICS AND INFORMATICS,Volume-3,Issue-4,Page(s):1- 9,2011.

[16] Safdar Ali Soomro, Sajjad Ahmed Soomro , Abdul Ghafoor Memo, Abdul Baqi,"Denial of Service Attacks in Wireless Ad hoc Networks", Journal of Information Communication Technology, Volume:4,Issue:2, Page(s): 01-10,2010.

[17] Fei Xing, Wenye Wang, "Understanding Dynamic Denial of Service Attacks in MobileAd Hoc Networks", Military Communications Conference, Washington, DC, DOI: 10.1109/MILCOM.2006.302178, ISBN:1-4244-0618-8,Page(s):1-7, Oct. 2006.

[18] S.B.Aneith Kumar S.Allwin Devaraj J. Arun kumar, "Efficient Detection of Denial of Service Attacks in MANET ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume: 2, Issue :5, ISSN: 2277- 128X, May 2012.

[19] Xiaoxin Wu, David K. Y. Yau, "Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach ", ASIACCS, March 20-22, 2007.

[20] Aditya Bakshi, A.K.Sharma , Atul Mishra"Significance of Mobile AD-HOC Networks (MANETS) ", International Journal of Innovative Technology and Exploring (IJ ITEE) ,ISSN:2278-3075,Volume:2,Issue:4,Page(s)-1-5,march 2013.

[21] Jian-Ming Chang , Po-Chun Tsou ,Han-Chieh Chao ,Jiann-Liang Chen,"CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic SystemsTechnology (Wireless VITAE) Chennai, DOI: 10.1109/WIRELESSVITAE.2011.5940839, Page(s)-1-5,Feb 28 2011-March 3 2011.

[22] Onkar V.Chandure, Prof V.T.Gaikwad " A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET" IJCSIT , Volume:2, Issue:6, ISSN:0975-9646,Page(s):2607-2613,Jul 2011.

[23] Vishnu K and Amos J Paul "Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" IJCA,ISSN:0975-8887, Volume:1, Isuue:22,Page(s)-38-42,Jan 2010.

[24] Megha Arya and Yogendra Kumar Jain "Gray hole attack and prevention in Mobile Adhoc Network" IJCA ,ISSN:0975-8887,Volume:27,Issue:10,Page(s)-21-26, Aug 2011.

[25] M. Medadian, M.H. Yektaie, and A.M. Rahmani." Combat with black hole attack in aodv routing protocol in manet. "Internet, AH-ICI 2009. First Asian Himalayas International Conference, Kathmandu ,DOI: 10.1109/AHICI.2009.5340351,page(s): 1–5, nov. 2009.

[26] Y.C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks in wireless ad hoc network routing protocols," in ACM Workshop on Wireless Security (WiSe), San Diego, California, USA,Page(s)-30-40, 2003.

[27] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir ,"Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation ",ICCIT, 2012.

[28] Rakesh kumar Sahu,Narendra S chaudhari "performance evaluation of ad hoc network under black hole attack" Information and Communication Technologies (WICT),Trivandrum, DOI:10.1109/WICT.2012.6409180, Page(s):780-784, Oct.3 2012-Nov. 2 2012.