IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VII (May-Jun. 2014), PP 93-101
www.iosrjournals.org

A Comparitative Survey on Malicious Nodes and Their Attacks in MANET

Ruchi Aggarwal[1], Simmy Rana[2]
[1, 2] *Department of Computer Sc. & Engg. , Chandigarh University, Gharuan, Punjab, India*

Abstract: *The designation of the mobile ad hoc networks (MANET) is, particularly to build up a dynamic wireless network, which has no antecedent and strictly defined infrastructure, within areas with limited or no available organized infrastructure, is possible for the parties to participate in MANET - authentic network users additionally as malicious attackers. This fact certainly raises the question regarding the protection. In this work we tend to concentrate on the common attacks within MANET, that differ in their essence like Sleep Deprivation attack, DoS etc. and what can be done as to stop them.*
Keywords*: MANET, AD-HOC network, Attacks, Protocols*

I. INTRODUCTION

A mobile ad hoc network (MANET) is an infrastructure less network of mobile devices. In MANET mobile devices communicate on network path for routing messages from one system to a different. In MANET all devices are liberal to move in any direction, and therefore change its links to other devices frequently. Every device should send traffic unrelated to its own use, and want to be a router. The main challenge in building a MANET is equipping every device to unendingly maintain the data needed to properly route traffic. These MANETs may operate by themselves or could also be connected to the larger Internet.

MANETs are a form of Wireless ad hoc network that typically includes a routable networking environment on top of a Link Layer ad hoc network. Lots of analysis has been applied in comparing MANET protocols using completely different parameters. These are focused on rising performance of MANET networks to consume energy with efficiency and routing more efficient. In ad hoc networks, nodes aren't familiar with the topology of their networks. Instead, they need to find it: a brand new node announces its presence listens for announcements broadcast by its neighbors. Every node learns concerning different close nodes and however to reach them, and make an announcement that it can also reach them.In MANETs, the nodes are mobile and battery operated. As the nodes have limited battery resources and multi hop routes are used over a changing network environment due to node mobility, it requires energy efficient routing protocols to limit the power consumption, prolong the battery life and to improve the robustness of the system[18].

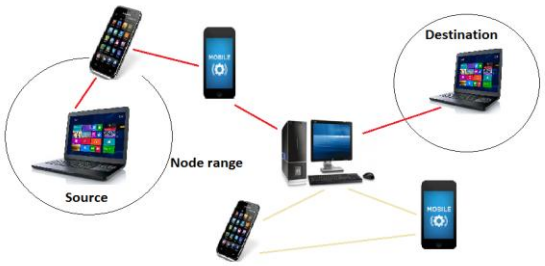

Fig1. MANET

A. MANET History

A MANET is a most promising and quickly growing technology that is based on a self-organized and quickly deployed network. Due to its great features, MANET attracts completely different real world application areas wherever the networks topology changes very quickly [22]. The main weaknesses of MANET are limited bandwidth, battery power, computational power, and security. Ad hoc networking isn't a brand new thought. As a technology for dynamic wireless networks, it's been deployed in military since 1970s. The recent IEEE standard 802.11 has enhanced the research interest within the field. Research in the area of ad hoc networking is receiving a lot of attention from world, industry, and government [22]. Since these networks cause several complicated problems, there are several open issues for analysis and development in this area.

1) Ad-Hoc Network

A MANET includes mobile nodes, a router with multiple hosts and wireless communication devices. Mobile ad hoc network are used for specific purpose. However ad-hoc network is preferred network because it's more versatile as compare to a different network .it is simply information transfer from one network to a different network, it increasing flexibility and consuming less time.

The characteristics and challenges of the MANET may be classified as: Cooperation-If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a legitimate and optimum chain of mutually connected nodes is created. This is called multi hop communication. Therefore every node is to act a host moreover as router. Ad hoc network don't have any pre-existing infrastructure. They are self-organized, self-configured, and self-controlled networks. This sort of network are often started or deployed anyplace and anytime because it poses terribly simple setup and no or lowest central administration. The network is characterised by the absence of central administration devices like base stations or access points [20]. Moreover, nodes are free to move in any direction, and thus can change its links to alternative devices often.

B. Routing Protocols

Routing Protocol is used to find valid routes between communicating nodes. They do not use any access points to connect to other nodes. It must be able to handle high mobility of the nodes. Routing protocols can be mainly classified into 3 categories:

1) Table Driven (Proactive) Protocol

Each node inside the network has routing table for the broadcast of the information packets and want to establish connection to completely different nodes inside the network. These nodes record for all the presented destinations and number of hops required to reach every destination inside the routing table. The routing entry is labelled with a sequence number that's formed by the destination node. To retain the steadiness, each station broadcasts and updates its routing table time to time. Every node contains the following information:

- How many hops are required to arrive that exact destination node.
- Generation of new sequence number marked by the destination.
- The destination address.

The proactive protocols are appropriate for fewer numbers of nodes in networks, because they need to update node entries for each and every node within the routing table of each node. It results a lot of Routing overhead problem. There is consumption of more bandwidth in routing table. Example: DSDV (Destination-Sequenced Distance-Vector), CGSR (Cluster gateway Switch Routing), WRP (Wireless Routing Protocol).

2) On-Demand (Reactive) Protocol

On-demand protocols, computes the routes and maintain routing information only if it is required and nodes establish routes only when required by the source. Route maintenance procedure helps in maintaining route information from source to destination. The routes are kept in routing memory of nodes as long as required. The route maintenance procedure was designed to overcome the wasted effort in maintaining unused routes. Reactive routing protocols sends out unnecessary messages to find the routes, they are not optimal in terms of bandwidth utilization, but they scale well in the frequency of topology change. Example: Ad Hoc On-Demand Distance Vector (AODV), Dynamic source routing (DSR), Location-aided routing (LAR).

3) Hybrid Protocol

Hybrid routing protocols include the benefits of each proactive and reactive protocols. This protocol is classified as a flat protocol due to overlapping of zones. As a result network congestion is sometimes reduced and best routes are usually detected. Each MN defines 2 zones: the within zone and also the outside zone. The hybrid protocols act as proactive protocols in the within zone and reactive protocols within the outside zone. Packets are broadcasted periodically in the within zone to create a routing table for all MNs in the within zone. When a node desires to send information to a destination node that resides within the outside zone, it uses a reactive protocol. Thus, a route discovery phase is invoked to determine the route to the destination MN. Example: ZRP (Zone Routing Protocol).

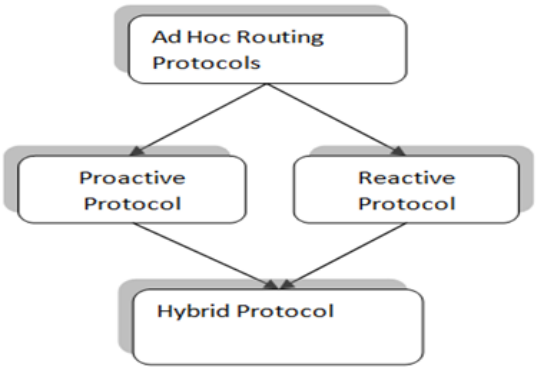

Fig 2.Routing Protocols

C. Types of Attack in MANET

Securing wireless ad hoc networks is a massive challenge. Before offering security in MANET or any ad hoc network, it is essential to understand probable kind of attacks. Ad hoc networks attack can be classified as inactive or active [17]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. The attacks can also be classified into 2 categories, namely external attacks and internal attacks, according the domain of the attacks. External attacks are carried out by nodes that don't belong to the domain of the network. Internal attacks are from compromised nodes that are actually part of the network. Internal attacks are more severe because an insider attack knows valuable and secret information, and possesses privileged access rights.

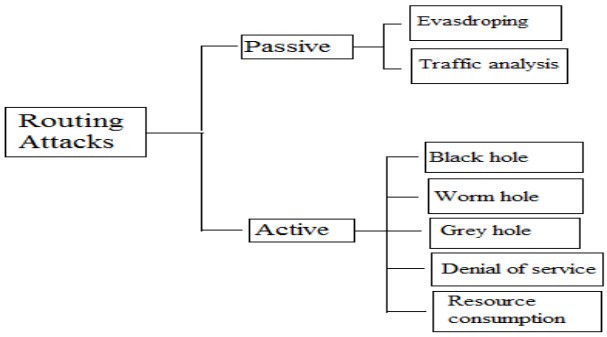

Fig 3.Security attacks

Active attack can be defined as "the attacker or fraud modify or alter the knowledge which may be shared among the nodes in the networks". The active attacks are usually launched by compromised nodes or malicious nodes. Malicious nodes change the routing data by advertising itself as having shortest path to the destination [17]. In MANET an attacker hurt the network performance by inappropriately modifying the routing message, injecting mistaken messages, or pretending a certified Mobile Node to confuse the traditional network.

Fig 4: Active attack

Black hole attack is a sort of attacks, malicious node claims having an optimum route to the node whose packets it desires to intercept. On receiving the request the malicious node sends a fake reply with very short route [17]. In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes alternative good nodes to route information packets through the malicious one. A malicious node drops all packets that it receives rather than normally forwarding those packets.

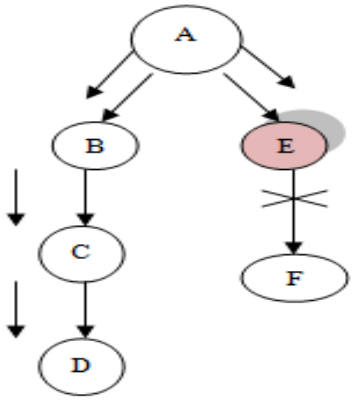

Fig 5: Black hole Attack

In Wormhole Attack, a wrongdoer receives packets at one point within the network, tunnels them to a different point in the network, and then replays them into the network from that point. Routing can be discontinuous once routing control message are tunnelled. This tunnel between 2 colluding attacks is known as a wormhole.

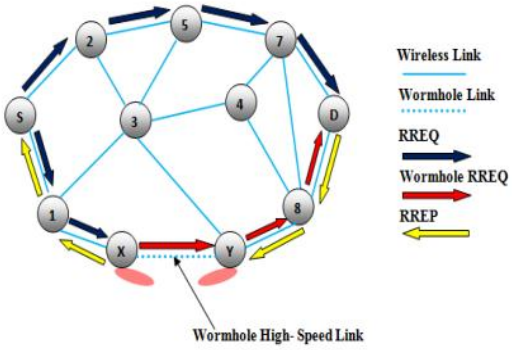

Fig 6.Wormhole attack [17]

Denial of Service aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker usually uses radio signal jamming and the battery exhaustion method. Gray-hole attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

In Resource Consumption Attack an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack. Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network [17]. It may include two important factors.

- Saving of battery power.
- Obtaining unfair share of bandwidth.

Modification, a malicious node modifies message throughout the transmission between the communication nodes, attackers modify packets and disrupt the overall communication between network nodes [17]. As an example, an attacker can deliberately shorten or lengthen the node list within the routing packet, lengthen the messages.

IP spoofing, malicious node sends a internet protocol packet containing its own Mac address and a victim's ip address, thereby usurping the IP-to-MAC address binding of the victim from the alternative neighbour's Address Resolution Protocol (ARP) cache.

In Tunnelling attack, a malicious node creates a very different kind of routing disturbance, known as tunnelling attack [19], and by using a pair of malicious nodes connected along via a private network connection [19]. Every packet received node A are forwarded to node B through their personal connection. This attack can most likely disturb routing by short circuiting the same old flow of routing packets. It implies that that if approved sender sends packets; it can be catched by personal network of trespasser being receiver so intruder send smashed packets to approved receiver.

Passive attack: it is an attack where an unofficial wrongdoer monitors or listens to the communication among two parties. It means that wrongdoer or intruder never send any corrupted message in a MANET network. A wrongdoer may inactively hear the network traffic to gather valuable data, like network connectivity, node location, traffic distribution, and so on. The main goal of passive attacks is to come up with threat against the network privacy [17]. Compared with active attacks, passive attacks are really powerful to prevent and find because the intruders aren't concerned in any modification of transmitted message or disruption of the network activity. Relying on dissimilar actions taken by an wrongdoer, passive attacks can be additional separated into following subcategories.

Eavesdropping: An assaulter will get direct data of the network by intercepting transmitted data packets. Passive eavesdropping may be prohibited by a range of encryption schemes and defensive the privacy of the data transmission, thus assaulter cannot acknowledge the encrypted data and it's key.

Traffic analysis attacks: AN attack might dig out valuable information from the distinctiveness of the transmission like node identity, the number of transmitted packets, time required to send one bit or a packet and also the frequency of data transmission. The extracted information may enable the wrongdoer to do an auxiliary analysis and decipher some sensitive information [17]. Traffic analysis in ad hoc networks might reveal following sort of info.

- Location of nodes.
- Network topology used for communication.
- Roles played by nodes.
- Available source and destination nodes.

II. RELATED WORK

Jian-Ming Chang et al. [1] presented a CBDS mechanism is that effectively detects the malicious nodes that attempt to launch gray hole/collaborative black hole attacks,using dynamic source routing technique. DSR involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network, it will reply with a RREP to the source node.

In S.B.Aneith Kumar et al.[2] This paper discuss Detection of Denial of Service Attacks in MANET. Due to lack of security, the network can be easily affected by several attacks. They are mostly vulnerable to the Denial of Service (DoS) attack because of its features. The new algorithm called reputation based system was developed, which detects and isolates the DoS attack and provides better misbehaviour detection.

In Bing Wu et al, [3] Author pro-vide a survey on attacks and countermeasures in MANET. Further defining countermeasures, are the features or functions which eliminate security vulnerabilities and attacks. Author gives an overview of attacks according to the protocols stack. According to the paper there are three ways to categorize the attacks. Firstly security attacks classification which is of two type first is Passive Attacks which consist Eavesdropping, traffic analysis, monitoring. Secondly Active Attack are Jamming, spoofing, modification, replaying, DoS. Secondly classification of attack is according to the protocol stack. All layers in the stack have different attacks individually. For example Black hole, Wormhole, Resource consumption is the Network layer attacks. Denial of service is Multi layer attack. Third type of attack is Cryptography Primitive Attacks like Digital signature attack, digital signature standard (DSS).Further author describes the security aware ad-hoc routing (SAR) protocol to defend the black hole attack which is based upon On demand protocols like AODV and DSR. A security metric is added into the RREQ packet, Intermediate nodes receive an RREQ

packet with a particular security metric. If the security metric is satisfied, the node will process the RREQ packet, otherwise, the RREQ is dropped. Author also provides defense against the two types of DOS attacks MAC layer and Routing layer attack. Routing layer attack is that malicious node reduces the TTL (time-to-live) field in the IP header so that the packet never reaches the destination. This may be countered by making it mandatory that a relay node ensures that the TTL field is set to a value greater than the hop count to the intended destinations. MAC layer DoS attacks is to Keep the channel busy and the battery life of that node may be drained. By avoiding the nodes that does not have the certificate of authentication the attack is prevented.

In Mohammad Al-Shurman [4] Author describes the "Black Hole Attack in Mobile Ad Hoc Networks". It presents two possible solutions. 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. Author studied only one node attack to be in the route (not a group of attackers). The group attack for this problem should be studied.

In Yi Tan et al. [5] The open paradigm of cognitive radio networks and lack of proactive security protocols, the IEEE 802.22 networks are vulnerable to various denial-of-service (DoS) threats. Author formulates the problem from both one-stage and a multi-stage scenario. In one-stage scenario, a cooperative game among the malicious nodes is formulated and derives the optimal decision strategy for them. In the multi-stage case, author propose a discrete-time Markov chain model for the dynamic behavior of both malicious nodes and the 802.22 secondary networks. In the multi-stage scenario, author incorporated the reactions of 802.22 secondary networks against the attacks and proposed a discrete-time Markov chain to model the change of states in a typical spectrum band. Further derived the expression for the net payoff as the system reaches steady state and proved it to be independent of the switching probabilities of the malicious nodes. As a result author showed that by taking the coordinated approach, the malicious nodes can obtain as high as 10-15% more net payoff than when they do not cooperate. And moreover, the numerical results for the multi-stage case indicate that when the system reaches steady state, there exist an optimal number of malicious nodes participating in the attack to achieve the maximum net payoff.

In Zhenqiang Ye, et al. [7] According to author It is important to provide redundancy in terms of providing multiple node-disjoint paths from a source to a destination, proposing a modified version of the popular AODV protocol that allows to discover multiple node-disjoint paths from a source to a destination. According to the author reliable nodes should be placed in the net-work for efficient operations. Simulation results show that the number of node-disjoint paths that can be found between a source and a destination depends on the density of nodes in the network.

In Nen-Chung Wang et al.[8] In this paper author propose an improved location-aided routing (ILAR) scheme to improve the efficiency of location-aided routing (LAR) scheme by using the global positioning system (GPS). They also propose a partial reconstruction process that maintains a routing path. When a node on a routing path finds that a link is broken, the node starts the process of routing maintenance. According to author for route discovery a baseline, is the line between the source node and the destination node. The request packet is broadcasted in a request zone based on the baseline to determine the next broadcasting node. The neighboring node with the shortest distance to the baseline is chosen as the next broadcasting node. Experimental results show that the proposed ILAR scheme good as compared to LAR scheme. It reduces the number of route discovery packets and increase the average route lifetime.

In Vasil Hnatyshin et al.[9] According to this paper LAR controls message overhead of Ad- hoc on-demand distance vector routing protocol by flooding only the portion that contain the route to destination. With the help of GPS it can find the possible location for destination node. From the Simulation results of OPNET Modeler version 16.0 the author concludes that LAR protocols generate significantly few control RREQ and RREP messages than AODV protocol.

In Elizabeth M. Royer et al.[10] According the author Route construction should be done with a minimum of overhead and bandwidth consumption. The main goal of an ad hoc network routing protocol is of correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. In this paper author examines routing protocols for ad hoc networks and evaluates these on the basis of given set of parameters.

In Guangyu Pei et al.[11] Author present a Fisheye State Routing which reduce routing update overhead in large networks. FSR is very flexible and maintain accurate routes MANET. Author compares the performance of FSR routing protocol with on demand routing protocols AODV and DSR. The Simulation result shows that FSR is more desirable for large mobile networks where mobility is high and the bandwidth is low.

In Maha Abdelhaq, [12] In this paper Author is concerned with studying sleep deprivation attack. The Intrusion detection algorithms, that is used in this paper is dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. DCA is Danger Theory based artificial immune system AIS intrusion detection algorithms. A mobile dendritic cell algorithm called MDCA is plugged with the DCA to find the attack. The proposed system MDCA has two subparts i.e. innate subpart and the adaptive subpart. According to author if the packet ID is found in detected list then it is rejected and an alarm is sent to that packet ID or if the

packet ID is found in alarmed list then the packet is also sent by an attacker so it is directly rejected, deleted from the routing table but without sending an alarm. Except the above two cases the packet analyzer analyze the packet ID. The task of packet analyzer is to generate the signals from the routing table and check availability of the bandwidth, and the power consumption rate. This information is stored in the signals stores. This antigen and signal store is the major source of input for DCA to detect the sleep deprivation attack over MANET. As a result MDCA is useful in early detection of two types of responses: it detects the danger very early especially when the same attacker comes again. Secondly, it broadcasting the IP address of the malicious node in alarm messages throughout the network, Which prevents the attack in the entire network.

In Bessy M Kuriakose et.al [13] According to author nodes that are infrastructure less, and have the ability to form a temporary network dynamically form a group of wireless ad-hoc network. Author says AODV is one of the commonly used routing protocols experiences a particular type of attack which is called the "Black Hole". Black Hole attack is called the packet drop attack. This is type of DoS attack. In this attack malicious node attracts all packets by falsely claiming that it is having the shortest route to the destination and then absorbs them without forwarding the packets. On behalf of the destination node the attacker node take advantage from captured message packets. Therefore malicious node send forged routing packets, to source to route packets from the source to itself. Further author describes the existing techniques to detect the malicious node. Author says that Intrusion Detection Systems is one of the most common techniques to detect the attacks. IDS can be stated as Network based (NIDS) or Host based. NIDS are setup on the data collection points like switches and routers. NIDS monitors traffic at these points and start scanning the traffic packet by packet, in order to try to identify the attack. In Route Confirmation Approach (RCA) the intermediate node send the route reply to source also send the confirmation route request to next hop and if it has the route it send the route reply to source node in order to confirm the validity of route. If both are the same, the source node confirms that the route is correct. But this technique cannot prevent the black hole attack if two malicious nodes work in sharing. Multiple Route Replies (MRR) the source node has to wait until an RREP packet comes from more than two nodes. Then if source node confirms that the route is safe and it can be used. As a result Time delay of packet increase. Statistical Anomaly Detection (SAD) can detect the black hole at low cost without launching extra routing traffic, and it does not require any modification of the existing protocol. Its drawback is that where the malicious node raises a false alarm indicating that a given condition has been fulfilled when it actually has not been.

In [14] Irshad Ullah et al. This paper discusses Black Hole Attack on MANETs Using Different MANET Routing Protocols with the help of Optimized Network Engineering Tool (OPNET). The impact of Black Hole attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both reactive and proactive protocols.

In Neha Kaushik et.al [15] The researcher have proposed many detection and prevention techniques for black hole attack whether single or cooperative. Thus, the state-of-art of these existing solutions are discussed and compared based on various parameters like PDR, throughput, end-to-end delay, routing overhead, etc. the problem for black hole attack is still an active field of research and researchers are working to combat this attack. In Jayshree Tajne et.al [16] Author discover multiple node disjoint paths with a low routing overhead during a route discovery, which also minimize the end-to-end delay and packet delivery ratio. Performance evaluated through simulation using .NET. In Jaya Jacob et.al [18] Author evaluates the performance of various adhoc routing protocols such as DSDV, AODV, DSR, TORA and AOMDV in terms of energy efficiency and it also proposes a new routing algorithm that modifies AOMDV and it provides better performance compared to all the above protocols. Simulation is done using NS-2(version NS-2.34).

In Varsha Patidar et.al [19] According to the author MANET is a hot research topic among researchers, due to the flexibility and independence of network infrastructure. The performance and reliability is break by attack on Ad hoc routing protocols. Nodes can leave and join the network at any time. A black attack is a severe attack that can easily employ against routing in MANET. This paper focus on various techniques on how black hole attack can be detect in AODV routing. Some solutions performed well in the presence of malicious node and protect the network from degradation. But some proposed solutions do not perform well due to the presence of multiple malicious nodes in the network. In AODV protocol, the route discovery process is vulnerable to Black Hole attack. So some efficient security method is needed to mitigate the effect of Black Hole Attack. In Sandeep Lalasaheb Dhende [20] According to author there are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. They present a technique to identify black attack and a solution to discover a safe route avoiding black hole attack. According to this proposed solution the requesting node without sending the data packets to the reply node at once, it has to wait till other replies. After receiving the first request it sets timer in the "Timer Expired Table", for collecting the further requests from different nodes. It will store the Sequence number, and the time at which the packet arrives, in a first Collect Route Reply Table (CRRT). As the solution the required security in MANET can

be achieved with minimum delay and control overhead and simultaneously we can detect the Black hole attack and transmit DATA packets to the destination.

TABLE I
Comparison of different techniques

Techniques	Authentication	PDR	Routing overhead	Energy consumption	End to end delay	Security	False positive rate
CBDS	No	Less	High	High	Less	No	
Reputation based system	Yes	Good	Better	Reduced			
Confidant approach	Yes	Packet forwarding is fixed per hop charges		Not concerned		Yes	
Multi-path routing and Packet sequence number comparison	Lower number of verified routes		No overhead in the channel because sequence number itself is included in every packet of base protocol		High	No	
ILAR-improved location-aided routing	No	Packet delivery rate of ILAR And LAR decreased when the speed increased.	Average	Normal		Yes	
GeoAODV	Yes		Adjusted	High	Assumed		
MDCA-mobile dendritic cell algorithm				Abnormal			Decrease
Multipath Routing Protocol		Good	Low		Minimize		
CRRT			Control		Minimum		

III. ATTRIBUTES IN MANET SECURITY

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

a) Confidentiality is to keep the information sent unclear to unauthorized users or nodes. MANET uses an open medium, so generally all nodes within the transmission mechanism range will obtain the data. One way to keep information confidential is to code the data, and another technique is to use directional antennas.

b) Authentication is to be ready to identify a node or a user, and to be able to stop impersonation [3]. In wired networks and infrastructure-based wireless networks, it's possible to implement a central authority at some extent like a router, base station, or access point. But there is not any central authority in MANET, and it's a lot of harder to certify an entity.

c) Integrity is to be able to keep the message sent from being illicitly altered or destroyed among the transmission. Once the data is distributed through the wireless medium, the data could also be modified or deleted by malicious attackers. The malicious attackers might also resend it, that's termed a replay attack.

d) Non repudiation is related to a proven fact that if an entity sends a message [3], the entity cannot deny that the message was sent by it. By manufacturing a signature for the message, the entity cannot later deny the message. in public key cryptography, a node A signs the message using its personal key. All completely different nodes can verify the signed message by using A's public key, and A cannot deny that its signature is hooked up to the message.

e) Availability is to keep the network service or resources offered to legitimate users. It ensures the survivability of the network despite malicious incidents.

f) Access control is to stop unauthorized use of network services and sys-tem resources [22]. Obviously, access management is tied to authentication attributes. In general, access management is that the most usually thought of service in both network communications and individual laptop systems.

IV. MANET VULNERABILITIES

a) Dynamic Topology- This means nodes can join and leave the network at any time, and move freely [18]. There is no fixed set of topology which reduces the network performance.

b) Lack of clear line of defence- Attackers can attack the network either internally or externally or from any direction. Because there is no clear line of defence.
c) Limited resources [18] - Set of devices used are laptops, computers, mobile phones. Each of them has different capacity of storing, power, speed.

V. CONCLUSION

As the survey is conducted in literature survey, we have come through the various techniques to detect various attacks. Thus there are vast numbers of techniques to detect attacks on MANET security. In [12] DCA technique is used to detect sleep deprivation attack. The Statistical Anomaly Detection technique can detect the black hole attack at very low cost and does not require any change in the existing protocol [13]. Multiple Route Reply causes increase in the time delay of packet which is the major drawback. Some techniques were strictly restricted to used to detect one malicious node. Now technique like Further Request approach is not suitable for cooperative attacks. As Intrusion Detection system is restricted to data concentration points like switches. Now we propose to adjust the CBDS approach to address other types of attacks on MANET like Sleep deprivation attack and DOS attack. Feasibility of implementing CBDS approach to integrate the security for these attacks.

REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE."Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" IEEE Systems Journal,2014

[2] S.B.Aneith Kumar, S.Allwin Devaraj, 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, May 2012Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei."A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless/Mobile Network Security, Springer, 2006

[3] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park. "Black Hole Attack in Mobile Ad Hoc Networks " ACMSE'04, April 2-3, 2004

[4] Yi Tan, Shamik Sengupta,Member, IEEE and K.P. Subbalakshmi,Senior Member, IEEE. "Analysis of Coordinated Denial-of-Service Attacksin IEEE 802.22 Networks" August 13, 2010

[5] Kemal Bicakci, Bulent Tavli, "Denial-of-Service attack s and countermeasures in IEEE 802.11 wireless network" ELSEVIER, 28 september 2008,pp- 931– 941

[6] Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks", IEEE 2003

[7] Nen-Chung Wang and Si-Ming Wang, "An Efficient Location-Aided Routing Protocol for Mobile Ad Hoc Networks" 11th International Conferenc e on Parallel and Distributed Systems (ICPADS'05), IEEE 2005

[8] Vasil Hnatyshin, Malik Ahmed, Remo Cocco, and Dan Urbano, "A Comparative Study of Location Aided Routing Protocols for MANET" IEEE 2011

[9] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" IEEE Personal Communications , April 1999,pp-46-55

[10] Guangyu Pei, Mario Gerla, Tsu-Wei Chen "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks" IEEE 2000

[11] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, "Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm" International Journal on New Computer Architectures and Their Applications (IJNCAA),The Society of Digital Information and Wireless Communications, 2011, pp-534-541

[12] Bessy M Kuriakose, M S Annie Ramya, "A Survey on Prevention of Black Hole Attack in an Ad-Hoc Network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 2, Issue 4, April 2013

[13] Irshad ullah, Shoaib ur rehman et al. "Analysis of Black Hole Attack on MANET Using Different MANET Routing Protocols " School of Computing Blekinge Institute of Technology June, 2010

[14] Neha Kaushik, Ajay Dureja, "A Comparative Study Of Black Hole Attack In MANET" International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 2, March – April, 2013, pp. 93-102

[15] Jayshree Tajne, Veena Gulhane. "Multipath Node-Disjoint Routing Protocol to Minimize End To End Delay and Routing Overhead for MANETs", International Journal of Engineering Research and Applications (IJERA),Vol. 3, Issue 4, Jul-Aug 2013, pp.1691-1698

[16] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANET on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT),Volume-1, Issue-5, June 2012

[17] Jaya Jacob, V.Seethalakshmi. "Performance Analysis and Enhancement of Routing Protocol in MANET", International Journal of Modern Engineering Research (IJMER) ,Vol.2, Issue.2, Mar-Apr 2012 pp-323-328

[18] Varsha Patidar, Rakesh Verma "Risk Mitigation of Black Hole Attack for Aodv Routing Protocol", IOSR Journal of Computer Engineering (IOSRJCE) Volume 3, Issue 3 (July-Aug. 2012), PP 12-15

[19] Sandeep Lalasaheb Dhende, Prof. D. M. Bhalerao "Detection/Removal of Black Hole Attack in Mobile Ad-Hoc Networks" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 6, August 2012

[20] Yu Liu, Cristina Comaniciu, Hong Man," A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", October14, 2006, ACM

[21] Priyanka Goyal, Vinti Parmar et al."MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.