A Review of Attacks on Ad Hoc on Demand Vector (AODV) based Mobile Ad Hoc Networks (MANETS)

[1]Aamir Mazhar Abbas, [2] Deepak P , [3]Lohith J J

[1 2] *UG student,*
, [3]Assistant Professor ,
[1 2 3] *Department of Computer Science & Engineering, BMSCE, Karnataka, India*,

Abstract— MANETs consist of mobile nodes that communicate with each other via radio waves using multiple hops to establish connections from the source to destination. Due to the inherent mobile nature of the nodes, routing these networks presents a challenge. Many researchers have designed and developed routing algorithm is, which have been classified into various categories, of which the most prominent classifications are proactive, reactive and hybrid.This paper presents a brief overview of the AODV protocol and the various types of attacks that can be performed on MANETs with a special mention to Flooding Attacks And Distributed Denial of Service Attacks.

Keywords—Wireless Network, Mobile Network, Ad-hoc Networks, Network Protocols, Routing Protocols, Network Security, and Attackers.

I. INTRODUCTION

Ad hoc mobile networks have the ability to be created on the fly, for one-time or temporary use. MANET's find special applications in military outfits and are an indispensable resource during disaster relief. The independent mobile nodes have a wireless interface to communicate with the other nodes using radio waves[1]. Nodes can communicate with other nodes directly when they are within the range, but require the aid of other nodes on the network to make communication possible between the nodes that are not directly connected to each other.

MANET's are formed for a particular reason, that is, to enable communication without the need for any pre-existing infrastructure[2]. Characteristics of ad hoc networks can be broadly classified as:

1) *Limited resources:* Networks are formed using mobile devices. Resources like battery-powered, bandwidth, computation power, memory etc have to be judiciously used in order to ensure the survival and proper functioning of the network. They are infrastructureless and the resources are limited.
2) *Lack of fixed infrastructure:* As these networks consist of mobile nodes, they cannot rely on any pre-existing infrastructure for their connectivity. These networks have the ability to configure themselves and to allow the nodesto move around freely and enter and leave the network according to their free will.
3) *Shared physical medium:* Nodes are free to move around within the confines of the network, without any limitations placed on them. All mobile nodes need to have access to the same wireless communication medium, with appropriate resources allotted to them. Therefore, access to the channel of communication cannot be restricted only to a few nodes.
4) *Dynamic topology:* Mobile nodes are not limited to a fixed location and their movement is not restricted in any manner whatsoever. The mobile nature of the entities of the networks means, the network should be dynamic in nature and have the ability to handle these scenarios, and balance out loads on-the-fly in order to ensure that the networks perform optimally.
5) *Autonomous nature of the networks:* The nodes of the network have the physical capability to communicate with other nodes only within a specified range. As the nodes are mobile in nature they are self-sufficient, in the sense that they are capable of routing application messages, ensuring that the network is secure and perform other functions. The need and complexities of infrastructure setup are eliminated by the inherent mobile nature of the networks.
6) *Economic viability:* When all the aforementioned qualities of ad hoc networks are combined, we see that beyond the initial setup, these networks prove to be very cost-effective by effectively eliminating the necessity of servers, the need to invest on physical cabling, routing devices, and all the costs that arise with the continual maintenance of the network on a daily basis.

II. MANET ROUTING PROTOCOLS

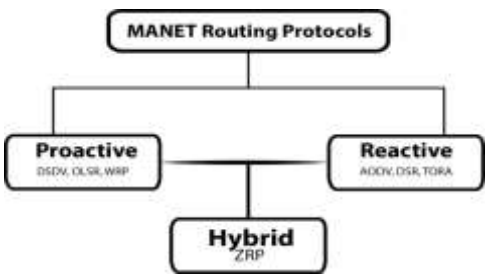

Figure 1 MANET Routing Protocol Classifications

In order to ensure successful communication between nodes, the node that is sending the message has to ensure that the receiver is within the transmission range of source[3].We assume that the mobile hosts use wireless radio-frequency transceivers as the network interface, and the range of the node is defined based on those specifications.
Communication can only take place when the source and receiver are within the radio range of each other. In MANETS, we assume that the mobile hosts use their wireless radio-frequency transceivers as the interface for the network, and the range of the node is defined as per the specifications.
Where two nodes are not able to communicate with each other directly, the intermediate nodes facilitate communication. For the network to be successful, all the nodes within the network should cooperate with each other, and we assume that all the nodes are cooperative. The mechanism according to which this communication happens is called routing and the set of rules that enable communication to happen is known as the routing protocol.
The nodes have the freedom to move around, and this will cause the network topology to change continuously. [4] The network should reflect these changes in connectivity, by mapping the various possible path from the sources to destinations within the network. Routing protocols will have to find a route from the source to destination and deliver the packets to the right destination. Their performance is directly related to the efficiency of the routing protocols employed to ensure the communication[5].
The efficiency of the routing protocols depends on several factors like

1) convergence after topology changes,
2) the bandwidth overhead that is incurred while enabling routing,
3) the battery capacity is and the rate of power consumption by devices,
4) the capability of the protocol to handle errors states except.

Figure 1 illustrates the prominent ways in which we generally classify MANETs routing protocols. The product classification is of two types, that is, Proactive and Reactive[6]. Another category of MANET routing protocols is derived from a combination of a combination of both proactive and reactive is generally referred as Hybrid protocols.
Proactive routing protocols: All the nodes in the network continuously search for routing information, and update each other about any of the new changes that are happening. The routing information of all the nodes is continuously updated with every change that happens in the network[7]. When any node needs to send a message to another node, the path is already known because every time a change happens in the network, it is broadcasted. Therefore the amount of time required to calculate the road before sending the packets (the latency of the network), is very low. But, in networks where the nodes continuously move, the maintenance and the continual subjugation of the topology information becomes a cumbersome task. As a result of which, the network in general suffers.
Reactive Routing protocols: In situations where there is a need for a path between two nodes and a message needs to be sent from a sender to receiver, then a form of query-reply dialog can be employed to make this happen. Here, a series of messages are sent to and fro from the sender to receiver, which perform various activities (such as setting up the communication, deciding on the means, authentication). Therefore, the latency is high; however, no unnecessary control messages need to be sent, ensuring that the overhead on the network is reduced substantially.
Comparison of the two: The network requires a certain amount of overhead, in order to ensure the efficient working of the network. In real-time, when communication needs to take place between entities of the network, the routes are readily available and the message can be passed on to the subsequent/intermediate nodes, without any delay that is incurred in finding out the route.
On the other hand, reactive protocols don't communicate with each other until and unless it is absolutely necessary. The only time when communication takes place is when some data needs to be sent from a source to destination. All the nodes in the network work together in order to obtain the routing information. The communication then takes place, after all of the routing information has been obtained. The network does not incur any overhead, as incurred by the proactive protocols, but on the flipside, there is a certain degree of latency and the route needs to be established to ensure communication.
Hybrid routing protocols: These protocols infuse the best qualities of proactive and reactive protocols and incorporate the merits of both. In the recent years, several hybrid routing protocols have been proposed like ZRP, ZHLS, SHARP and NAMP and a variety of routing protocols and comparative analysis of the routing protocols have been performed either using of simulation results or analytically .

III. AODV ROUTING PROTOCOL

A. Introduction to the AODV protocol

The Ad-hoc On-Demand Distance Vector(AODV) routing protocol is designed to be used in ad-hoc mobile networks, and is reactive in nature, meaning that routes are created between source and destination only when they are [10]. Each routing reply is assigned a sequence number to determine whether routing information is up-to-date and to prevent loops and routing.
Query and reply cycles are used as the basis of route discovery. When a node requires a route to a particular node it sends a routing request to its neighbors and when a route has been found the reply will be sent back to the originator of the message. Please keep in mind, that each node does not essentially maintain the whole routing information[11]. The nodes only need to remember the destinations and the appropriate next hops in the route with some auxiliary information. Therefore, AODV is a typical distance vector routing algorithm. Four types of control packets are used:

a. Routing request messages (RREQ)
b. Routing reply message, which is routed back to the source of the RREQ
c. Route error message (RERR), which is used to notify the other node of the loss of link, or loss of message, which is common mobile networks
d. HELLO messages which are sent periodically to detect and monitor the links to the neighbors

B. Overview of the routing protocol

Every node on the network stores its own routing table, and every entry includes the following items:

1. a destination
2. number of hops that lie on the route
3. destination sequence number
4. a list of nodes that can forward packets on the route
5. the expiration time for this particular table entry

Every node performing AODV protocol maintains a sequence number that is incremented when it sends a RREQ or when the destination node sends back the RREP message[12]. This sequence number is used to distinguish the up-to-date route from the route that existed previously, which could possibly be invalid. Thus, AODV is completely loop free and copes well in a highly dynamic network.

Every node on the network that is taking part in performing AODV maintains a sequence number which is incremented every time an RREQ is sent or when a reply is sent back from the destination node. This sequence number is used to distinguish the older routes from the routes that are up-to-date, which enables AODV to cope well and dynamic conditions and keeps the whole network loop free.

When messages have to be sent to a node on the network, which is not a direct neighbor to the sender, it will broadcast a RREQ message[13]. When a message is received, the fellow nodes will try to satisfy the request by doing the following:

1) If a valid route is present in the routing table, or if the neighboring nodes is the destination, an RREP message will be sent back to the node that sent the request.
2) If a valid route does not exist, the message will be rebroadcasted.

The RREQ ID will be incremented every time the sender sends a new RREQ, which enables the unique identification of an RREQ by using a combination of the source IP address and request ID. By using this method, all the other nodes in the network can discard the duplicate and the older RREQ messages. This reduces the overhead incurred during broadcasting. If a link breaks down and is detected by one of its neighbors, the neighbor will generate a RERR error message, which will delete the route that points to the lost neighbor. All the routes that pass through this node, also have to be modified to reflect the changes. This is done by determining if any of the neighbors are affected, and then delivering an appropriate RERR to those neighbors.

C. Sequence numbers

The removal of old and invalid information requires the use of sequence numbers. Sequence numbers work or perform the functions of time stamps, which prevents the protocol from the loop problem[11]. Every destination host has a sequence number stored in the route table, which is updated when the host receives the message with a greater sequence number.

Every node is responsible for maintaining its own sequence number, and changes in one of the cases:

1) The value is incremented before sending RREQ message.
2) Value is changed before the destination node sends a reply RREP in response to the request that it received. Every node must update its own sequence number till it reaches the maximum value possible.

D. Evaluation of AODV

The main advantage of AODV is that we do not need to setup a Central Administrative system to manage, control and optimise the routing process. The protocol reacts very well to changes in the topology of the network, and saves storage space and energy because each node is only responsible for storing the routing entries which it is responsible for, or is interested in to send[14].

On the other hand, the disadvantage of this protocol is that valid route might expire and it is more often than not hard to determine or generalise expiration time. If we set an expiration time that is too short, it will cause repeated, unnecessary routing requests. But, if we set the expiry time to be too long, it will slow down the protocol and the time the network needs to react to reflect the changes in topology.

As the protocol is used with mobile nodes, it is designed in such a way that it stores only a very limited amount of information with each node, that is information regarding the destination, next hop and a few important details. As all the devices are mobile devices, they have a limited range, which causes AODV to rely on the route discovery flood more often. This might result in a significant network overhead.

The performance of the protocol is poor in larger networks, as large networks have longer paths, and an implication of which is that the certain parts are more vulnerable to link breakages and requires a substantial amount of control overhead for its maintenance[11]. At the same time, AODV is vulnerable to many kinds of attacks, as the protocol is based on the assumption that all the nodes on the network are good and will always cooperate to ensure the efficient working of the network.

IV. ADVANTAGES OF MANETS

MANETs generally use economically viable devices and are setup on demand. Other than this, the advantages of ad hoc networks include the following:

1) Decentralised administration makes the networks very robust and the networks need to react to changes in topology in a very short span of time.
2) All nodes in the network are free to move around within the confines of the network, and can join and leave the network whenever required. This leads to improved flexibility for all the nodes involved.
3) All nodes are provided access to the information on the services of the network, irrespective of what the geographical position within the network might be.

4) The networks are self configuring. This eliminates the need for physical cabling and configuration of the network devices.
5) The networks are open to other devices joining in. After the setup of the network, it can be scaled to whatever size required, to meet the requirements of the network.

V. SECURITY ISSUES

MANET's and their inherent mobile nature sets new challenges for working professionals and researchers in the field of network security[15]. Mobile networks are susceptible to many different kinds of security threats, and this section gives a brief overview of the product classification of these problems.

1) Nodes acting as routers: The nodes themselves are responsible for delaying in propagating the messages in the network. Malicious nodes can take advantage of this and misuse the messaging traffic by generating false messages, dropping packets etc
2) Limited resources: Mobile ad hoc networks operate under very limited network resources. Using methods that require elaborate cryptographic solutions that are applied to wired systems where the resources are not limited, cannot be applied to mobile networks directly.
3) Medium of communication: Communication between nodes is done using wireless media. This implies that, any message that is broadcasted in the network can be accessed by all nodes on the network (malicious or not), and the sender has no control over it.
4) The location of the nodes:As ad hoc networks are formed to serve a purpose, in situations where infrastructure does not exist, it cannot be guaranteed that the networks will be security sensitive.
5) No predefined boundary: We cannot precisely define the physical boundary of the network, as the mobile nodes are allowed to move within the physical constants of the network. No restraints placed on which node can join, and leave the network. As soon as a malicious node comes within the radio range of other nodes within the network, it can communicate with them, and join the network.

The inherent mobile nature of mobile ad hoc networks implies that security constraints must be considered, taken seriously and implemented. A few of them are described below:

1) *Confidentiality:* We must ensure that methods are implemented to prevent access of any part of the information from unauthorized entities while the data is being transmitted. Depending on the type of application, the ad hoc networks may face consequences if confidentiality is not setup properly.
2) *Authenticity:* The network must ensure that all the nodes in the network are either genuine or trusted node is. If authentication is not properly implemented, malicious nodes on the network can deceive the genuine nodes, and can gain access to confidential information.
3) *Availability:* Networks are built to enable nodes or entities on the network to successfully exchange data with each other. When any node joins and network, it expects to have reasonable access to the network resources. This constraint can be violated by a distributed denial of service attack.
4) *Integrity:* When a message is sent from a sender to receiver, the message should reach, or be delivered to the receiver without any external modification. Modification of the original message results in the violation of an integrity constraint. The network should be able to ensure that unauthorised entities do not have the capability of modifying and corrupting any messages sent by genuine nodes.
5) *Non-repudiation:* This constraint ensures that every node takes responsibility for its actions and, cannot deny the actions that were performed by itself. This property ensures that faulty nodes are detected and thus, helps in isolating them from the network.

VI. CATEGORISING NETWORK ATTACKS

Attacks in mobile ad hoc networks are broadly classified on the basis of how the attacks are performed. That is, if the attacks are active or passive[16].

A. Active attacks

Active attacks require the continual and active participation of the attackers. The attacker generates tamper with the network resources, by causing congestion, propagating wrong routing information etc. As the attackers are active on the network, their detection and prevention is done using suitable prevention algorithms. A few examples of active attacks are impersonation, fabrication, message replay and modification attacks

B. Passive attacks

Passive attackers don't want to bring down the network to a standstill, but are there to steal information. In order to do so, they do not perform any actions that might make them stand out from the rest of the nodes. The do not disturb the normal functioning of the network, and simply become a part of the network. Being a part of the network enables them to continuously keep an eye on the happenings of the network and gain access to the network traffic, in turn violating message confidentiality constraint. As the nodes do not initiate any malicious activity, which results in the disruption of the normal functioning of the network, it is very difficult for us to identify such attacks and pinpoint the nodes that are the attackers. A few examples of these types of attacks are eavesdropping, traffic analysis and monitoring.

Another classification of the types of attacks on the network is on the basis of the position of the attacker, with respect to the network[17]. That is, whether if the attacker is external to the network or is an integral/internal part of the network.

A. External attacks: attacks made by unauthorised nodes that are not a part of the network, and are external to the network are known as external attacks. These attackers fled bogus packets in the network, aiming to cause congestion in the network and breakdown the normal day-to-day functioning.

B. Internal attacks: these attacks are performed by nodes that are already authorised and are part of the network. The nodes can have selfish reasons for their malicious behaviour. The reasons could be:

a) Saving resources: the nodes might want to protect their resources like battery power, processing capabilities and the bandwidth that the using for communication. This kind of attackers would like to take advantage of other nodes and utilise their resources for personal benefit.

b) Hijacking: attackers will hijack the nodes that are already authorised and are part of the network, and in turn use those nodes to launch internal attacks in the network.

VII. ROUTING ATTACKS

A. Flooding attack

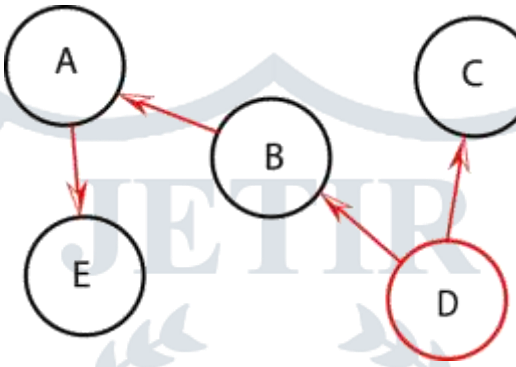

Figure 2 Example of Flooding Attack

Flooding attack of the most basic form of Denial of Service(DoS)[18]. The aim of flooding attack is to paralyse the whole network, by exhausting the available resources of bandwidth, battery power on the nodes etc. The most common methods of performing flooding attack is by using radio jamming signals and by using techniques that cause the nodes to utilise computation power resulting in battery exhaustion. Let us illustrate one variation of the attack.

1) Consider a simple network consisting of 5 nodes, addressed A, B, C, D, and E. Here, node D is the malicious node and generates request packets destined to the node address H. But, node edge does not exist in the network.
2) D broadcasts request packets to all of its neighboring nodes, that is nodes C, node G and node E. Nodes which is not a direct neigh Therefore, these nodes in turn forward the packets to their neighboring nodes.
3) None of the neighbors will be able to find node H, because it does not exist in the network, and will therefore broadcast again assuming that some other nodes may be able to find the path to it.
4) If mechanisms are not implemented to ensure that malicious packets are not continually forwarded in the network, the nodes will keep forwarding the packets which will result in loss of battery power and wastage of bandwidth and will result in flooding.

As illustrated above with RREQ packets, malicious node can also perform flooding by using data packets. In this technique, after the node has established itself as an entity on the network, it starts sending useless data packets to other nodes in the network.
Flooding attacks can be detected in the following ways:

1) We can detect malicious nodes by using the help of genuine nodes in the network. When a node sends RREQ packet, it suggests and neighbors take the responsibility of maintaining a check on the rate of packet generation. If the rate in which the packets generated exceeds predefined threshold value, which is either set numerically or is decided dynamically by the algorithm implemented, the node responsible for generating the packet is put onto a blacklist and that information is broadcasted throughout the network.
2) In the same manner, to detect data flooding, a threshold value is also specified for all nodes in the network and its value is periodically checked by the neighboring nodes.

A few methods that have been proposed categorised all system nodes as strangers, acquaintances and friends depending on the trust level that has been calculated by using various parameters like ratio of packets forwarded to the total number of packets sent to the neighbor, ratio of packets received two the total number of packets that have been deceived without any modification etc. By ranking each of the nodes according to their trust level, that is, by utilising numerical values to do not the trust level, a few relationships have been proposed which can be generalised into the following model:
trust threshold (friend) > trust threshold(acquaintance)> trust threshold(stranger)

B. Sleep deprivation attack

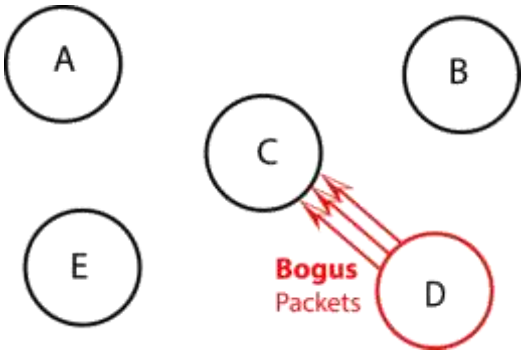

Figure 3 Illustration of a Sleep Deprivation Attack

Attackers implement sleep deprivation attacks by forcing the targeted node or the targeted group of nodes to use their vital resources like battery power, network bandwidth and the computing power available to them by sending false requests for either existent or non-existent nodes[19]. This is a form of flooding attack where the targeted node is exhausted resources, and are unable to be a part of the network. While the targeted node is receiving bogus packets in messages, it will have a hard time processing the requests that are coming from genuine nodes as all of its resources are dedicated towards processing the majority of the bogus packets that it is receiving. Thus, the victim node is unable to process the routing mechanism and when it runs out of power, it becomes unreachable by other nodes in the network.

In the figure illustrated above, node D is a malicious node and continually sends bogus packets to node C. C, on the other hand receives all of the bogus packets that are sent towards it, and begins to process each one of them. Meanwhile, when packets are sent to B from the other genuine nodes on the network, it takes time for node C to process all of them and send replies back to the genuine nodes. This, in turn results in a form of denial of service to the other genuine nodes. Over a period of time, node C utilises all of its resources processing the bogus data and packets which it received from D, and when it's battery resources are over, the node gets eliminated.

A few of the solutions proposed to overcome the sleep deprivation attack are as follows:

1) Clustering based prevention mechanism has been proposed bySarkar et al. in [18], and suggests that the node with the lowest node identification number be assigned as the cluster head. The cluster head gets updated everytime to cluster heads come in direct contact with each other. It is the cluster heads responsibility to forward packets for a particular source destination pair to all the nodes within its cluster until it reaches a threshold value. After this, the cluster head breaks its connection with those nodes. This prevents a node from sending excessive traffic.

2) Another solution has been proposed by Bhattasali et al. [19] and uses a hierarchy based model for the detection of sleep deprivation attacks. The network is logically broken and divided into clusters, of which its cluster is headed by a cluster in charge (CIC). The CIC initiates data collection request and the collected data is sent to a sector in charge (SI C). It is the SICs responsibility to forward this data to the leaf nodes of the network. The leaf nodes process this data and returns the results to the SEC, which in turn forwards the collected data to the sector monitor (SM). The CIC takes the final decision to prevent the rate of false positive detection and forwards all of the valid data to the sink gateway (SG), along with the rejected invalid data. The SG also adds the suspected nodes onto and isolation list for further prevention.

C. Rushing attack

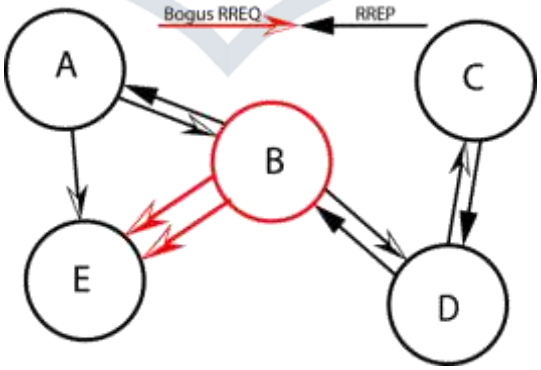

Figure 4 Example of Rushing Attack

Rushing attack suggest that the attacker will try and become a hop in the path to the targeted node[20]. When a route requests are forwarded, the malicious nodes forwards the RREQ's faster than the authorised nodes to increase the probability that the routes that are discovered will be one of the route that includes the attacker[21]. Thus, the attacker can thus tamper the message traffic passing through it. Let us illustrate this type of an attacks using an example:

1) The attacker floods its neighboring nodes with bogus request RREQ packets so as to slow down the processing speed. In the above scenario, node A requests for a route to node C by sending route request packets. Node B, which is playing the

role of a rushing node in the above example, receives the RREQ request and sends bogus packets to node E. Node Eis a genuine node on the network and should have been a part of the route from A to C. But by giving bogus information to A, node B is able to react to the route request from A to C faster than E is able to react and sends a reply back before E can. Therefore, node B is able to enter the route from A to C and gain access to all the packets that are being sent to C.

2) Another way of doing this is when an attacker speeds up its route request packet transmission rate by transmitting them at higher transmission power, thereby decreasing the number of hops required to reach the destination. By using this method and transmitting in a range that is much larger than the range of the other nodes, the malicious node is genuinely able to create routes that are much shorter than the standard lengths of the route from the network.

D. Impersonation attacks

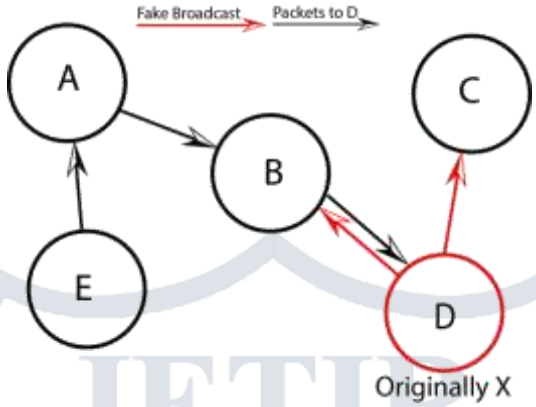

Figure 5: Example of Impersonation

Let us illustrate the general working of an impersonation attack. Consider a network scenario as denoted in figure 5. Here, node X sends packets to its neighbors, that is nodes C and node B, by using the source address as node D. As node X has convinced all the network entities that it is node X, all the packets coming to destination D from node C and B will now be received by node X, which is impersonating itself as node D.

E. Routing table poisoning attack

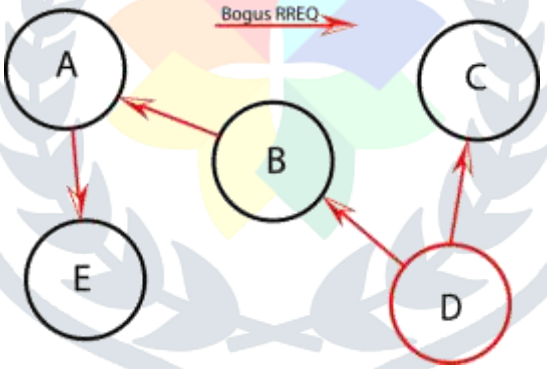

Figure 6An Example of Routing Table Poisoning Attack

Malicious nodes corrupts the routing tables of other nodes in the network, by altering information, which results in the creation of false routes, suboptimal routes, loops and causing congestion in certain parts of the network[23]. Poisoning of routing tables can be done in the following ways:

1) the attacker broadcasts false traffic and thus creates bogus entries in the table is maintained by other nodes on the network.

2) The attacker generates route request packets whose sequence numbers are higher and result in the deletion of legitimate routes which had low sequence numbers.

Consider the network scenario denoted in the diagram, where node D is a malicious node and corrupts the route in tables of nodes C, G and E. This results in the formation of loops in the network. SEAD protocol makes use of a one-way hashing chain to prevent malicious nodes from increasing the sequence numbers or decreasing the hop counts in the route in packets. The usage of different hash function is ensures that the attacker will never be able to design a lower metric value or greater sequence value.

VIII. CONCLUSION

This paper presented a brief overview of the classification of routing protocols used in MANET's. This paper presents the kind of attacks that these networks is able to and presented a number of popular attacks like the flooding attack, the sleep deprivation attack, the black hole attack, the route in table poisoning attack and the impersonation and rushing attacks along with some of the proposed solutions. Many of the issues that need to be addressed keeping in view the security concerns of the mobile ad hoc

networks have also been highlighted. There is an urgent need to detect and prevent these attacks in a timely fashion, and we would like to proposea security system which perform the analysis of AODV based mobile ad hoc networks for presence of a malicious nodes and propose methods to prevent flooding attacks by excluding the same from the system.

IX. ACKNOWLEDGEMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this report. A special gratitude we give to our Principal Dr. MallikarjunBabu and our Head of Department, Dr. Guru Prasad.
A special thanks goes to our guide, Mr. Lohith J. J, who has invested his full effort in guiding our team in achieving the goal. We have to appreciate the guidance given by other supervisor as well as the panels, especially in our project presentation that has improved our presentation skills; thanks to their comment and advices.

X. REFERENCES

[1] Aarti et al., International Journal of Advanced Research in Computer Science and Software Engineering, May - 2013, pp. 252-257 "Study of MANET: Characteristics, Challenges, Application and Security Attacks"- Volume 3, Issue 5.
[2] M Bansal, R Rajput, G Gupta - The Internet Society, 1999
[3] EM Royer, CK Toh - -Personal Communications, IEEE (Volume:6 , Issue: 2) ISSN :1070-9916
[4] David A. Maltz et al; MobiCom '98 Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - Pages 85-97 - ISBN:1-58113-035-X
[5] S. Corson, J. Macker - "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations" - 1999 RFC
[6] A. P. Janani et al; "A competitive performance analysis of reactive and proactive routing protocols of MANET under short time communication scenario" - International Journal of Wireless and Mobile Computing , Volume 6 Issue 3
[7] KahkashanShaukat, Violet R. Syrotiut - "Locally proactive routing protocols" -ADHOC-NOW'10: Proceedings of the 9th international conference on Ad-hoc, mobile and wireless networks - Pages 67-80
[8] Hyun-GonSeo, Ki-Hyung Kim et al; "Performance of service location protocols in MANET based on reactive routing protocols" - ICN'05 Proceedings of the 4th international conference on Networking - Volume Part II - Pages 234-241
[9] Antoine B. Bagula - Computer Communications archive - Volume 29 Issue 7, April, 2006 - Pages 879-892
[10] Perkins, C.E, Royer, E.M. - "Ad-hoc on-demand distance vector routing" - Second IEEE Workshop on Mobile Computing Systems and Applications, 1999. - 25-26 Feb 1999 - Page(s) 90 - 100
[11] Abdallah, A.M. et al; "Analysis of a defenseless ad hoc on demand Distance Vector routing protocol under routing disruption attacks" - The 7th International Conference on Informatics and Systems (INFOS), 2010 - Page(s) 1 - 5
[12] Peter Höfner et al; "A rigorous analysis of AODV and its variants" - ACM 2012 - MSWiM '12 Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems - Pages 203-212
[13] ZafarMehmoodKhattak, MuddesarIqbal, Xingheng Wang - "A Comparative Performance Study of Ad Hoc Routing Protocols to Improve the Route Discovery Process of AODV" - International Journal of Adaptive, Resilient and Autonomic Systems - Volume 5 Issue 4, October 2014 - Pages 20-33
[14] Zongwei Zhou - "Security enhancement over ad-hoc AODV routing protocol" - CNIS '07 Proceedings of the Fourth IASTED International Conference on Communication, Network and Information Security - Pages 116-121
[15] PengNing, Kun Sun - " How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols" - Ad Hoc Networks - Volume 3 Issue 6, November, 2005 - Pages 795-819
[16] Stacy Prowell, Rob Kraus, Mike Borkin; Seven Deadliest Network Attacks - Syngress Publishing ©2010 - ISBN: 9781597495509
[17] Simon Hansman, Ray Hunt; "A taxonomy of network and computer attacks" - Computers and Security archive - Volume 24 Issue 1, February, 2005 - Pages 31-43
[18] YinghuaGuo, Sylvie Perreau; "Detect DDoS flooding attacks in mobile ad hoc networks"- International Journal of Security and Networks archive - Volume 5 Issue 4, December 2010 - Pages 259-269
[19] Hahnsang Kim, Joshua Smith, Kang G. Shin - "Detecting energy-greedy anomalies and mobile malware variants" - MobiSys '08 Proceedings of the 6th international conference on Mobile systems, applications, and services - Pages 239-252
[20] Yih-Chun Hu, Adrian Perrig, David B. Johnson; "Rushing attacks and defense in wireless ad hoc network routing protocols" - WiSe '03 Proceedings of the 2nd ACM workshop on Wireless security - Pages 30 - 40
[21] Hyojin Kim et al; "A Novel Robust Routing Scheme Against Rushing Attacks in Wireless Ad Hoc Networks" - Wireless Personal Communications: An International Journal archive - Volume 70 Issue 4, June 2013 - Pages 1339-1351
[22] Michel Barbeau , Jyanthi Hall, EvangelosKranakis; "Detecting impersonation attacks in future wireless and mobile networks" - MADNES'05 Proceedings of the First international conference on Secure Mobile Ad-hoc Networks and Sensors - Pages 80-95
[23] Imran Raza, S. A. Hussain; "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes" - Computer Communications - Volume 31 Issue 9, June, 2008 - Pages 1796-1802