ISSN(Print):2320–9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

Survey of Attacks on Wireless Network

Ankur Bawiskar[1], Dr. B.B. Meshram[2]

Student, Dept. of Computer Technology, Veermata Jijabai Technological Institute, Mumbai, India[1]

Head of Department, Dept. of Computer Technology, Veermata Jijabai Technological Institute, Mumbai, India[2]

Abstract*:* Wireless networks are gaining popularity to its peak today, as the users want connectivity in terms of wireless medium irrespective of their geographic position. There is an increasing threat and various attacks on the Wireless Network.The main aim of this paper is to provide a survey of wireless network and attacks that occur on it. This paper also provides an overview of routing protocols being used in wireless networks. It also discusses the attacks on access point in wireless network. Ad-hoc network must have a secure way for transmission and communication which is quite challenging and vital issue. Ad-hoc network are rapidly gaining popularity because they do not rely on a pre-infrastructure and can be deployed spontaneously. Application of ad-hoc network ranges from offices to modern battlefields. Security is a serious concern in wireless networks due to its open nature of communication.

Keywords*:* AODV, DSR, Denial of Service, Ns2, Trace File

I. Introduction

Communication being a mode of sending and receiving information is gaining more popularity in today’s world. There are various modes of communication one of them is wireless mode; in which communication takes place through an open medium. There are various types of wireless networks. These are cellular networks, satellite networks and ad hoc mobile networks. Amongst the wireless networks 802.11 networks are the most popular. Wireless 802.11 networks can be categorized into two types: Infrastructure and Ad-hoc mode. Infrastructure based networks have a fix backbone. An ad-hoc network is a collection of nodes which can communicate with each other without any infrastructure. Wireless medium is a medium which can be accessed by both legitimate users and attackers. End users and corporations are heavily interested in taking the advantage of this wireless medium, but this also comes with some security issues.

In this project we will be studying the routing protocols in ad-hoc network using the ns2 simulation tool. Another aim is to implement attacks on access points and also attacks on network layer in ad-hoc network. These attacks are carried out using backtrack cd and also by implementing tcl scripts in ns2 simulation tool. The last module includes the detection of attack by analyzing trace file generated by ns2 simulation tool.

II. Wireless Network Architecture and Components

A. Architecture for Wireless Lan

Wireless technologies today come in several forms such as Wireless PAN, Wireless LAN and Wireless WAN. These networks have their own characteristics and properties. Wireless PANs are those networks in which interconnected devices communicate using either ZigBee or Bluetooth. The range for these is very less i.e.10m. Wireless LANs are those networks that have various devices capable of communicating with each other. The devices possess the wireless adapter cards. The 802.11 series of Wireless comes into this category.

Figure 1 shows the architecture for the wireless network and can be explained as follows. There are two access points having their own coverage area. There are some clients/devices that are associated with the access points. The Access point 1(Dept1) is having three laptops associated with it. The Access point2 (Dept2) is also having three laptops associated with it. These access points are connected to a switch which in turn is connected with the router. The router provides the internet services to the clients.

The general architecture of wireless Lan can be shown as follows:

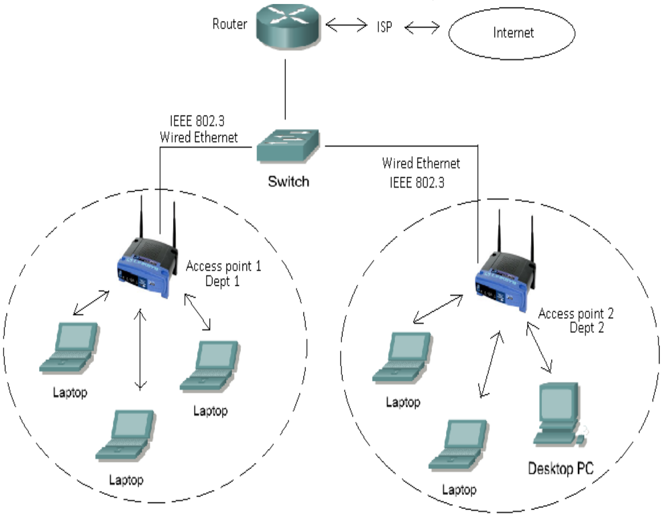


Fig 1 Architecture of WLAN

B. Components of wireless network

Wireless LANs consist of components similar to traditional Ethernet-wired LANs. In fact wireless LAN protocols are similar to Ethernet and comply with the same form factors. The big difference, however, is that wireless LANs doesn't require wires. The components of wireless network can be described as below in figure 2:

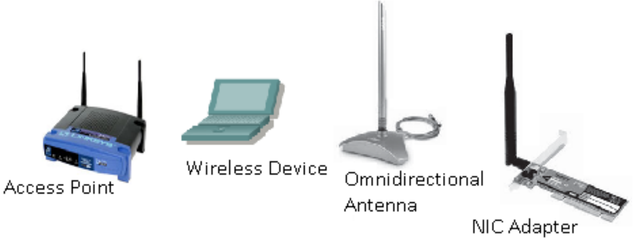


Fig 2 Components of WLAN

- Access Point: An Access point operates within a specific frequency spectrum and uses an 802.11 standard modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. It converts Ethernet frame to 802.11 frames.

- Wireless Network Interface Cards: A PC or workstation uses a wireless NIC or client adapter to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates it to an AP or another wireless client. The cards generally implement one particular physical layer, such as 802.11a or 802.11b/g/n. It also uses a particular frequency such as 2.4GHz or 5GHz.

- Antenna: An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omni directional), gain, transmit power, and so on. Antennas are needed on the APs, bridges, and clients. Antennas for 802.11b and 11g networks, operating in the 2.4 GHz ISM band.

- Wireless Devices: Users of wireless LANs operate a multitude of devices, such as PCs, laptops, and PDAs. Laptops and PDAs, however, are commonly equipped with wireless LAN connectivity because of their portable nature. Nowadays most of the devices are having the inbuilt feature of possessing wireless nic card to enable them to get access to the wireless network anywhere and anytime.

- Miscellaneous Devices: There are many other miscellaneous devices used in wireless network such as routers, bridges and repeaters. A typical wireless LAN router includes four Ethernet ports i.e. an 802.11 access point. Wireless LAN routers offer strong benefits in the home and small office setting. Wireless repeaters, however, are a way to extend the range of an existing wireless LAN instead of adding more access points. Wireless bridges are used to connect multiple LANs (both wired and wireless) at the Media Access Control (MAC) layer level. Used in building-to-building wireless connections, wireless bridges can cover longer distances than APs.

III. ADHOC NETWORK

A. Introduction

Wireless LANs can be classified based on their mode of operation such as either infrastructure or ad-hoc. Infrastructure mode has a fixed wired backbone for communicating with each other; whereas the ad-hoc mode doesn't rely on a backbone. An example of formation of ad-hoc network can be of sensor nodes present in an open atmosphere. In this network each sensor node has the capability of processing the information available to it from the atmosphere and capable of sharing this information with other nodes. A practical application of the ad-hoc wireless sensor network is sharing climate information such as humidity, temperature, etc at high altitude pilgrimage place.

B. Adhoc network characterisitcs

An ad hoc network can be formed when a group of mobile devices communicate with each other without depending on any fixed infrastructure [11]. In such cases, neighboring nodes communicate with each others while communication between non-neighbor nodes is performed via the intermediate nodes that can act as routers. The network topology also frequently changes in ad-hoc network. Ad-hoc wireless networks are prone to route breaks that can result due to various sources such as node mobility, signal interference, high error rate and packet collision [11].

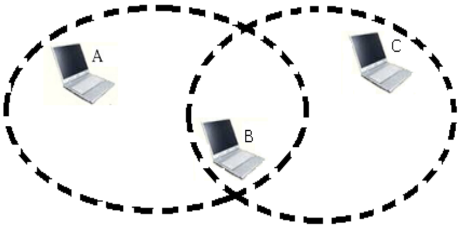


Fig 3 Ad-hoc network

The above figure 3 explains the adhoc network wherein there are three nodes A,B and C. Node A and Node B are in the range of each other. Similarly node B and C are in range of each other. If node A wants to send some data to node C it has to pass through the intermediate node b so node B acts as a router. Here comes the main operation of routing in adhoc network.

C. Routing in Adhoc network

Routing in an adhoc network is the most important task that needs to be handled with care. Since nodes in adhoc network depend on intermediate nodes in carrying of the data so there are various routing protocols used in this process. The main aim of routing protocols in an adhoc network is to find minimum hop distance between source and destinatin with minimum overhead and bandwidth [6]. Depending on the routing topology being used they are classified as : proactive, reactive and hybrid.

- Proactive Protocols: In proactive protocol each node present in the network has information of complete topology [6]. The tables are updated constantly so that they contain fresh enough information for routing.

- Reactive Protocols: In reactive protocol nodes create path on an on-demand basis. Information about the network topology is collected only when it is required. This avoids the overhead associated with frequent updation of routing table in each node in the network [6].

- Hybrid Protocols: In hybrid protocols group of nodes are formed and then the nodes are assigned different functionalities inside and outside the group. Grouping is done based on position of nodes [6].

D. Reactive Routing Protocols

Amongst the type of routing protocols; reactive routing protocols are the most widely used because of their lower overhead in sharing of routing information. The two main reactive routing protocols used are AODV and DSR.

- AODV- Adhoc on-Demand Distance Vector

AODV is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other [3]. This routing protocol uses two phases. In phase 1 route discovery is done. In phase two route maintenance is done. It uses three control messages namely RREQ, RREP and RRER[2]. The RREQ and RREP messages are used in phase1 whereas RRER control message is used in phase 2.

The steps to be followed in AODV protocols are as follows:[2]

i. Source node broadcasts RREQ message. It contains source and destination address, sequence number and broadcast id.
ii. If the next node is the destination then it replies with RREP message or else message is forwarded to next node.
iii. When forwarding the RREQ message node maintains broadcast id, source address and maintains a reverse route.
iv. Sequence number helps in route updation and also helps in getting fresh enough route to the destination.
v. Destination node on receiving RREQ then sends a unicast RREP message to the source node on the same path that was created during RREQ.

The procedure can be shown in a diagrammatic view as follows in figure 4 and 5: [6]
Route Discovery-

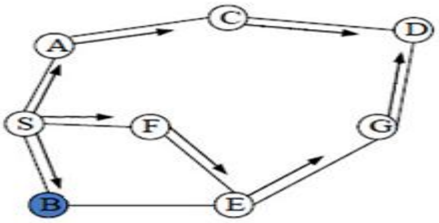


Fig 4 RREQ Message

Route Reply-

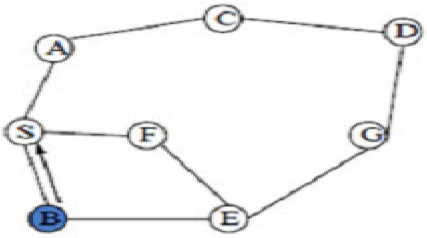


Fig 5 RREP Reply Message

- DSR- Dynamic Source Routing

Dynamic source routing is a reactive routing protocol which is able to handle the dynamically changing topology. It is called as source routing because each data packet contains the complete list of nodes that the packet should traverse to reach destination. It also operates on two steps: Route Discovery and Route maintenance [5]. Source node uses route discovery to find path to destination. It also uses control messages such as RREQ, RREP.

The steps to be followed in DSR protocol are as follows: [5]

i. Source node broadcasts RREQ message. It contains source and destination address, sequence number and broadcast id.
ii. If the next node is the destination then it replies with RREP message or else message is forwarded to next node.
iii. When forwarding the RREQ message node maintains broadcast id, source address and maintains a reverse route.
iv. The Destination then sends a RREP message in reverse direction.
v. On receiving the RREP message the source records the route in its cache for future use. Intermediate nodes also store this information.
vi. Route maintenance mechanism is used to notify the source node about possible change in network topology.

IV. THREATS AND VULNERABILITIES IN WIRELESS NETWORK

Wireless networks possess various vulnerabilities that can lead to various attacks on them. The wireless networks consist of three basic components: transmission using radio frequencies, access point that provides connection to clients and the users [7]. Each of these components possesses some vulnerability that provides a way of performing an attack. There are various issues to be handled in wireless ad-hoc network such as shared physical medium, no central management, limited resources and dynamic topology.

The vulnerabilities in wireless network can be considered using two components: access point and routing protocols.

A. Vulnerabilities in Wireless Devices

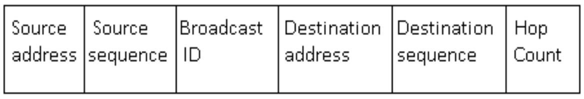
There are various vulnerabilities to the wireless devices such as access point, client devices. These vulnerabilities can be described as belows:

- Battery Powered Operation: Wireless devices such as laptops, PDA and other devices are battery powered. Even a little sharing of information incurs a great amount of power loss. This is a serious threat as devices cannot be equipped with more power.
- Limited Computational Capability: The devices/nodes in wireless networks possess very limited computational power. These devices are capable to handle less memory operations.
- Dynamic Topology: The nodes in an ad-hoc network have dynamic topology so it is very difficult to keep track of node's position for the purpose of information sharing.

B. Vulnerability in Routing Protocols

The routing protocols used in wireless networks are those that are used in ad-hoc network. These are Aodv and Dsr. Routing protocols are more susceptible to attacks because in ad-hoc network the important task of sharing information is handled by intermediate nodes. The intermediate nodes cannot be guaranteed to be a legitimate one. The vulnerabilities in routing protocols can be explained as belows:[1]

- Vulnerability in AODV- The AODV protocol is most widely used in ad-hoc network for routing. The AODV uses RREQ and RREP messages. The format of RREQ message which can be shown in figure 6 is as follows:[6]



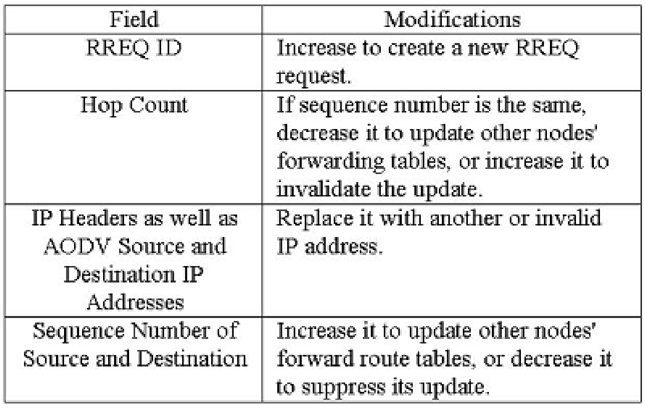
Source address	Source sequence	Broadcast ID	Destination address	Destination sequence	Hop Count

Fig 6 RREQ packet header

The fields in the AODV RREQ message can be easily modified to carry out an attack. The RREQ message can be tampered to propagate false message in the network. Similarly the RREP message can be tampered to reroute the traffic and send false reply to source node [1].

The vulnerable fields in AODV routing messages along with the modification required can be shown in table 1 as belows:[1]

Table 1 Fields and modifications in aodv



Field	Modifications
RREQ ID	Increase to create a new RREQ request.
Hop Count	If sequence number is the same, decrease it to update other nodes' forwarding tables, or increase it to invalidate the update.
IP Headers as well as AODV Source and Destination IP Addresses	Replace it with another or invalid IP address.
Sequence Number of Source and Destination	Increase it to update other nodes' forward route tables, or decrease it to suppress its update.

- Vulnerability in DSR: The DSR protocol also possess some vulnerability such as: corrupting route request packet, spoofing route replies, malicious routing query to non-existent nodes.

V. ATTACKS IN WIRELESS NETWORKS

Wireless networks are more susceptible to attacks because of their shared physical medium, open transmission of radio frequencies [5]. The attacks on wireless networks can be studied based on two phenomena i.e. attacks on access point and attacks on tcp/ip protocol stack. We will first study the attacks on access point and then the attacks on tcp/ip stack. The attacks on wireless networks can be shown in diagrammatic manner in figure 7as belows:

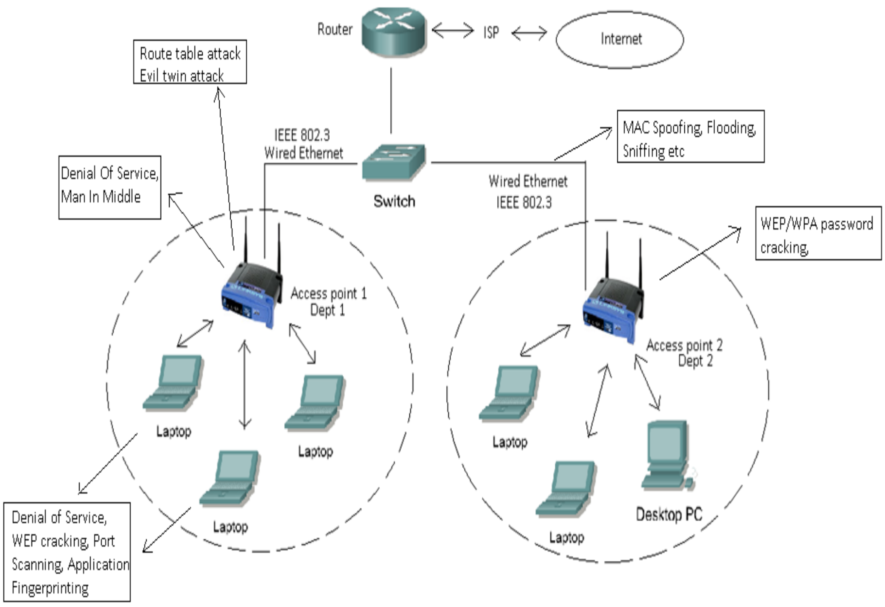


Fig 7 Attacks in WLan

The attacks in wireless network can be classified into two types: passive attack and active attack.

- Passive Attack: The passive attacks are those which do not harm the network, but they only perform network reconnaissance. They try to get valuable information from the network by snooping the traffic.

- Active Attack: The active attacks are those attacks in which the attacker modifies the data or performs some malicious activity that disrupts the network or causes disconnection.

A. Attacks on Access Point

The access point is an important wireless device that becomes vulnerable to an attack. It provides services to the clients that get associated with it. It has SSID, encryption key, etc. There are various attacks on an access point. They are as follows:

- Password Cracking- In this attack an attacker gathers the encryption key associated with the access point and after getting associated with the access point can perform snooping and sniffing of the traffic that passes through the access point. It leads to unauthorized access. The attacker uses set of tools available in the backtrack penetration operating system to perform this attack.

- Fake Access Point- In this attack an attacker uses the same SSID as that of the real AP and forces client devices to connect to this fake AP. This allows the attacker to analyze all the traffic passing through this AP. This is shown in figure 8.

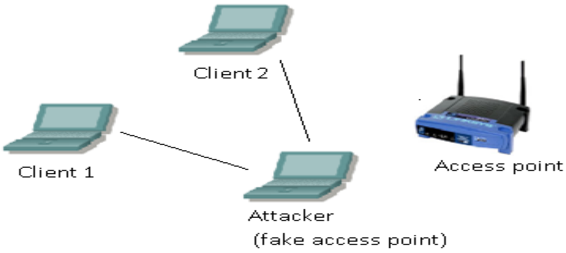


Fig 8 Fake access point

- Packet Injection- In this attack an attacker using some utility injects huge amount of data packets to the access point. Due to this the access point is unable to serve to the clients that are associated with it. The clients get disconnected from the access point as the access point is unable to handle huge data packets. This can be shown using figure 9.

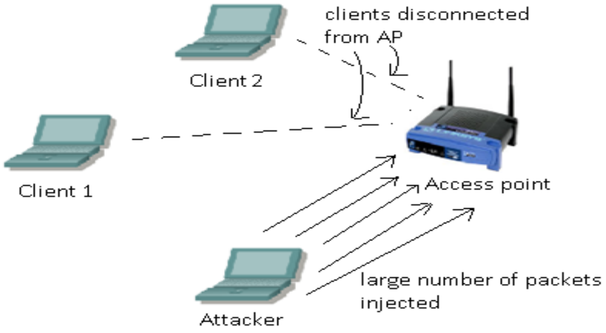

clients disconnected from AP
Client 2
Client 1
Access point
large number of packets injected
Attacker

Fig 9 Packet Injection

- Denial of Service- In this type of attack the attacker sends large number of de-authentication packets to the access point that causes the clients associated with the AP to disconnect from the AP. This can be done using the ‘airplay-ng ‘utility. It can be shown by below figure 10.

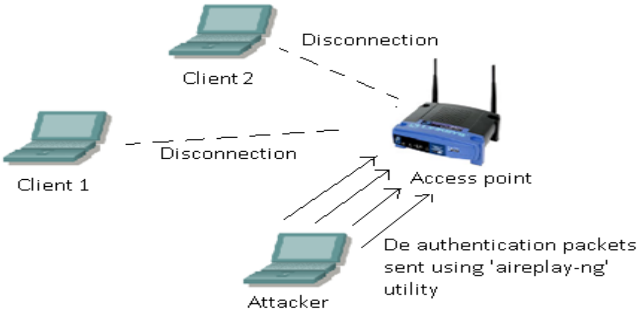


Fig 10 De-authentication Packets

B. Attacks on Tcp/ip layers

Attacks on wireless networks can also be classified based on the layer on which they occur [5].There are attacks on application layer, transport layer, network layer, link layer. These attacks can be explained as below using table 2:

Table 2 Tcp/ip Attacks

Layer	Attacks
Application	DoS, Worms, CSRF, SQL Injection, Viruses
Transport	Session hijacking, Covert channel
Network	Flooding, Packet Dropping, Denial-of-service
MAC Layer	Signal Jamming, Sniffing

- Application Layer: Application layer is responsible for running the services. The attacks that are made on this layer include running malicious scripts, virus and worms.

- Transport Layer: Transport layer is responsible for maintaining the session information between two communication devices. Session hijacking can occur that can lead to an attacker taking over the session of legitimate client.

- Network Layer: Network layer attacks are those attacks that take place due to the vulnerabilities in routing protocols. Attacks on routing can be named as routing table overflow, flooding attack.

- MAC Layer: Medium access is an important issue due to the open medium of radio frequencies in wireless networks. Various attacks such as signal jamming can lead to DoS. Sniffing can also be done in promiscuous mode.

B. Attacks on Routing Protocols

Routing protocols are used by both the source nodes and the intermediate nodes in ad-hoc network. The two most commonly used routing protocols are AODV and DSR. Attacker can launch a single attack in which many fields of AODV are modified or an aggregate attack consisting of multiple attack messages [1].

The examples of single attacks are those in which a single field of AODV is being modified to perform an attack.

- Forging Sequence number: The sequence number field in AODV messages indicates the freshness of the route to the particular node. A packet with large sequence number is generally accepted because it indicates fresh route. An attacker can exploit this vulnerability. Attacker sends a reply message with large sequence number and it causes the victim node to pass through its own node. The forging of sequence number can be explained with a diagram as follows using figure 11:[8]

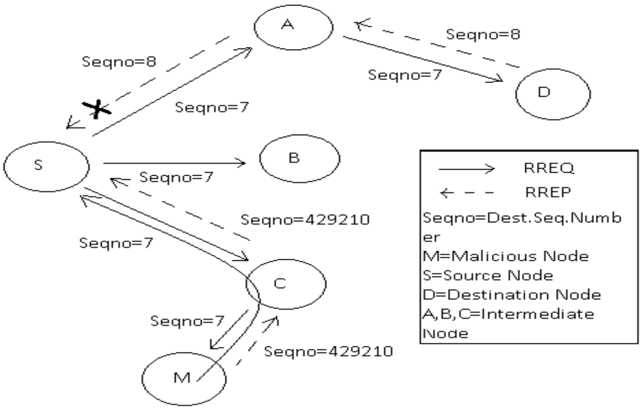


Fig 11 Sequence Number modification

In the above scenario the nodes A, B, C are intermediate nodes, whereas node S is source node, node D is destination node. Node M is malicious node. Node M sends a reply message with large sequence number and forces source node to send data through it.

- Sleep Deprivation: Every node in ad-hoc network requires a battery to send and receive signals from it. The devices transmit signals only when there is a need to do so. An attacker can send large number of route request messages so that these devices process it and thereby reduce the battery of the devices.

- Flooding Attack: In this attack the attacker sends large number of route request packets. Generally there is a limit on number of route request packets to be sent in a network. But the attacker surpasses this number and floods the network with large packets, thereby disrupting the services in the network.

- Denial of Service: The ad-hoc network contains nodes in the network. Some of the nodes can be malicious nodes. The malicious nodes are those nodes that drop packets completely or selectively. It causes denying of the service to the legitimate nodes. The denial of service attack is a serious attack on the ad-hoc network because the legitimate nodes are deprived of the services in the network.

C. Existing methods for mitigating attacks

There are many existing mechanisms to prevent and detect such type of attacks on routing protocols. Some of them are as follows:

- Trust Based method: One of the methods used is based on trust value calculation of redundant control messages. The trust score of the neighbor node will be calculated by evaluating the duplicate control packets received from that node. Initially all the nodes in the network will be assigned with a trust value (T). Further the trust value of a node will increase if it is a benevolent node (T+1) and the trust value of a node will decrease if it is a malevolent node (T-1) [12].

- Two-Ack scheme: TWOACK mechanism has been proposed at network layer as a scheme. When a node forwards a packet to its next hop, it verifies whether the packet has been successfully received by the node that is two hops away down the route [13]. This is achieved by a special type of acknowledgement packet called TWOACK, which stores a fixed route of two hops in the opposite direction to the data packet. This scheme can be added into a source routing protocol such as DSR. It has a limitation that as each data packet has to be acknowledged along the route, this generates considerate amount of overhead and degrade the network performance.

VI. APRROACH AND METHODOLOGY

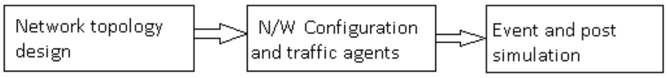
The main aim is to study the routing protocols in ad-hoc network using the ns2 simulation tool. There are three modules in the project namely: Routing Protocol module, Attack module and Detection and Prevention module. In this section first of all ns2 simulation tool will be explained followed by the three modules in the system along with the diagram.

A. NS2 tool

The simulation tool most widely used for the wireless network is the ns2 simulation tool. NS- 2 is the second version of a popular network simulator intended for wired networks. It was developed and created by the Virtual InterNetwork Testbed project (or VINT). This second version is extended by the possibility to simulate wireless networks. NS- 2 is an event based simulator, which means that simulation is following a timeline with several pre defined events on it. It can be downloaded from the website- http://www.isi.edu/nsnam/ns/ns-build. html.

B. Routing Protocol Module

The routing protocol module is used to study and analyze the routing protocols used in ad-hoc network. The simulation is done using the ns2 simulation tool. The block diagram for this module can be shown as belows:


Network topology design
N/W Configuration and traffic agents
Event and post simulation

In general, a simulation scenario consists of three main components:

- A network topology
- Connections, traffic and agents (protocols)
- Events and failures

- **Network topology design:** A network topology defines number of nodes and their connectivity, and can either be created manually. Connections and traffic are set up by traffic generators and agents (protocols) at a node. In this step we define the trace file and network animation procedure.

```
#Open the Trace file
set tracefile1 [open out.tr w]
$ns trace-all $tracefile1
#Open the NAM trace file
set namfile [open out.nam w]
$ns namtrace-all $namfile
```

- **Configuring and running simulation:** This step implements the design specified in the first step. In this step network configuration is done such as which protocols to be used i.e. tcp or udp. This step maintains the simulation clock and generates a trace file that can be further analyzed.

```
$ns duplex-link $n0 $n2 100Mb 5ms DropTail
set udp [new Agent/UDP]
$ns attach-agent $n0 $udp
# Start the simulation
$ns run
```

- **Event and post simulation:** The main tasks in this step include verifying the integrity of the program and evaluating the performance of the simulated network. In this step the trace file generated by the ns2 is also analyzed to understand the packet formats and types.

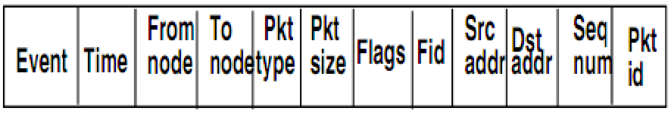
C. Attack module

The second module can be defined as Attack module. In this module the various attacks such sniffing and obtaining user credentials, denial of service, packet injection are being performed. The attacks against the access point are also being carried out. The attacks are implemented using the backtrack cd and also by writing scripts in ns2 tool. The ns2 tcl script coding is used to perform some attacks and these are simulated using the ns2 simulation tool.

D. Detection and Prevention module

The third module can be defined as detection and prevention module. In this module the steps to prevent attacks done against the access point will be described. It also contains the analysis of the ns2 trace file to detect attack in the network.

- Ns2 trace file format: Whenever a ns2 tcl script is run a trace file is generated that describes the packet formats and types being used in simulation. Understanding of this trace file is very important in identifying the attack happening on the network. The ns2 trace file can be described as follows in figure 12:[10]



Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addr	Dst addr	Seq num	Pkt id

Fig 12 Ns2 Trace file Format

The file format can be explained as belows:

1. **Event**-The first field is the event type. It is given by one of the four possible symbols r, +, -, d which correspond respectively to receive, enqueued, dequeued and dropped.
2. **Time**-The second field gives the time at which the event occurs.
3. **From node**-The third field gives the input node of the link at which the event occurs.
4. **To node**- This field gives the output node of the link at which the event occurs.
5. **Packet type**- This field specifies the packet type (for example CBR or TCP). This name depends on the type of packet specified in the scripting file.
6. **Packet size**- It gives the packet size in terms of bytes.
7. **Flags**- It specifies the flags being used in the packet format.
8. **Fid**- It specifies the flow id of the IPv6 that a user can set for each flow at the input OTcl script. It can be used for further analysis purposes.
9. **Source address**- This specifies the source address in the form of “node.port”
10. **Destination address**- This specifies the destination address in the form of “node.port”
11. **Sequence number**- This is the network layer protocol’s packet sequence number.
12. **Packet id**- This field identifies the unique id of the packet.

VII. Conclusion

Wireless networks are gaining more and more popularity in today’s world because of their many benefits and applications. Because wireless communication use open medium for sending and receiving data they are more susceptible to attack. Wireless ad-hoc networks have more security threats as they solely rely on the nodes present in the network. Routing is an important issue that needs to be handled with care in ad-hoc network. In this paper we have discussed some threats and vulnerabilities in wireless and ad-hoc network. This paper provides us with an insight of attacks done on wireless networks. This paper can act as a basis for understanding of wireless and ad-hoc network and also attacks occurring on them.

References

[1] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko,” A Specification-based Intrusion Detection System for AODV”, Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks, pp.125-134, 2003.

[2] Sreedhar. C, Dr. S. Madhusudhana Verma and Dr. N. Kasiviswanath,”Potential Security Attacks On Wireless networks and Their Countermeasure”, International Journal of Computer Science & Information Technology (IJCSIT), Vol.2, No.5, pp. 76-89, October 2010.

[3] Nital Mistry and Devesh C Jinwala, ”Improving AODV Protocol against Black hole attacks”, Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol II, March 2010.

[4] Dr. M.S.Aswal, Paramjeet Rawat, Tarun Kumar”, Threats and Vulnerabilities in Wireless Mesh Networks”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, pp. 155-158, November 2009.

[5] Shalini Jain and Dr.Satbir Jain,” Detection and Prevention of Wormhole attack in mobile Ad hoc networks”, International Journal of Computer Th eory and Engineering, Vol. 2, No. 1, pp.78-86, February, 2010.

[6] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, ” Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA, Vol.2, No.1, pp. 45-54, February 2012.

[7] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, " Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, pp. 77-86, July 2008.

[8] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan," Mitigation of Black Hole Attacks for AODV Routing Protocol", pp. 336-343.

[9] Christian Barnes, Tony Bautts, Donald Lloyds (2002), "Hack Proofing Wireless Network", Syngress Publishers, USA.

[10] Eitan Altman and Tania Jimenez,"NS Simulator for beginners: Lecture notes", pp. 27, 2003-04.

[11] Ahed M. Alshanyour, Uthman Baroudi, "Bypass AODV: Improving Performance of Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol in Wireless Ad Hoc Networks" , Paper Published in ICST and Ambi-sys, February 2008.

[12] A.Pravin Renold, R.Parthasarathy, " Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks", International Conference on Advances in Computing, Communications and Informatics (ICACCI) ACM, pp. 1271-1275, August 2012.

[13] Nan Kang, Elhadi M. Shakshuki, Tarek R. Sheltami, " Detecting Misbehaving Nodes in MANETs", Proceedings of iiWAS ACM, pp. 216-222, Nov 2010.

BIOGRAPHY

Ankur Bawiskar received his B.E. degree in Computer Engineering from University of Mumbai. He is currently pursuing his M.Tech degree in Network Infrastructure Management System from VJTI, Matunga, Mumbai, INDIA.

Dr. B. B. Meshram is working as professor in Computer technology Dept, VJTI, Matunga, Mumbai, INDIA. He is Ph.D. in computer Engineering. He has taught various subjects such as Object Oriented Software engineering, Network Security, Advanced Computer Network (TCP/IP), Data Warehouse and data mining, etc at Post Graduate level. He has guided several projects at graduate and post graduate level. He is life member of CSI and Institute of Engineers.