Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Ad-hoc Networks

Ranjana Sharma, Vishal Dogra, Aftab Khan
B.Tech, SSGI,KUK University
India

Abstract— Adhoc means innovation which is used to describe things that are created randomly, mostly for a single use. It is also called node-to-node wireless network that is used for sharing Internet Connection between terminals. Adhoc network is Multi-hop radio relaying network. It has been further categorized into infrastructure based network and infrastructure less networks. In infrastructure based network communication occurs directly with access points between nodes. When wireless network is created then wireless adapter starts broadcasting. Administrative cost got reduced in these networks. Ease of deployment is there. This paper mainly focused upon the architecture, working principle, classifications, and attacks of adhoc networks.

Keywords— Active attack, Adhoc Network, Denial of Service, Infrastructure based, Infrastructure less.

I. INTRODUCTION

. First adhoc network was Packet Radio Network (PRNet) research initiated by DARPA in 1972 with the recognization of Packet Switching. PRNet shared broadcast radio channel in many radios efficiently but had low throughput. An adhoc network is a combination of more than two devices equipped with wireless communications and capabilities of networking. It allows anywhere, anytime computing. This setup is adaptive and self-organizing. It supports both peer-to-peer communication and peer-to-remote communication.

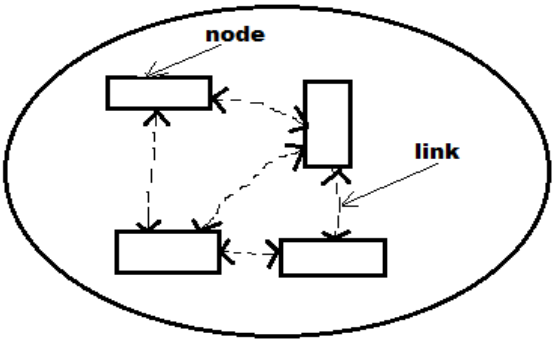

Fig 1. Architecture of Ad-hoc network diagram

An Ad hoc network can be divided into homogeneous network (all devices are identical, have same features and capabilities) and heterogeneous network (neither devices are identical nor have same capabilities) on the basis of nodes. As if all mobiles or computers like nodes are connected, then network is homogenous otherwise heterogeneous.

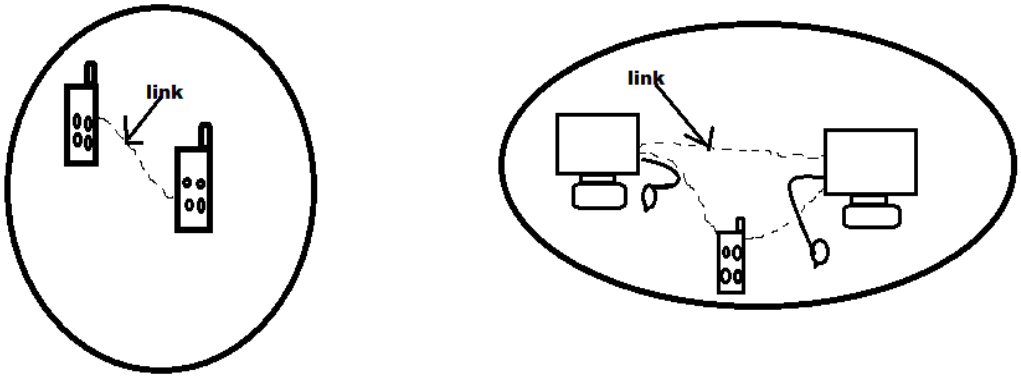

Fig 2. Homogeneous and Heterogeneous adhoc network

The Paper is structured as follows: Working Principle of adhoc network is discussed in section II. In section III, types of adhoc network is introduced and section IV, presents a brief overview of attacks in adhoc networks.

II. WORKING PRINCIPLE:

In adhoc networks, node A communicates with B in the channel. This makes a single-hop network means there is only direct communication between server and client no other node is there. One other type of network is there i.e multi-hop network which is used when channel is not available. One intermediate node should be there which acts as router (like C in figure iii), for routing the packets.

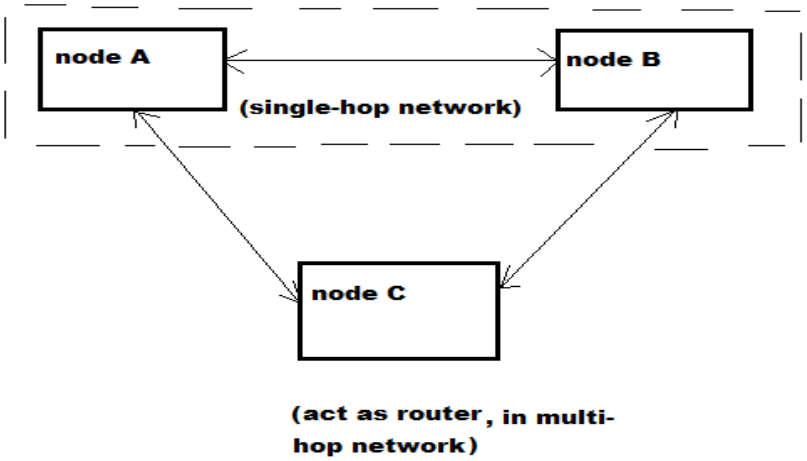

Fig 3. Multi-hop network containing a single-hop network

III. TYPES OF ADHOC NETWORKS:

A. *Infrastructed networks*:

This network is fixed infrastructure based. Wiring is there between equipments. This network can be implemented on areas where access points can be easily placed. Communication is done using fixed access points. Cellular network is the example of this type of network. Centralized routing is done mainly. During handoff, low call drops. Time synchronization is achieved easily. High cost of maintenance is required.

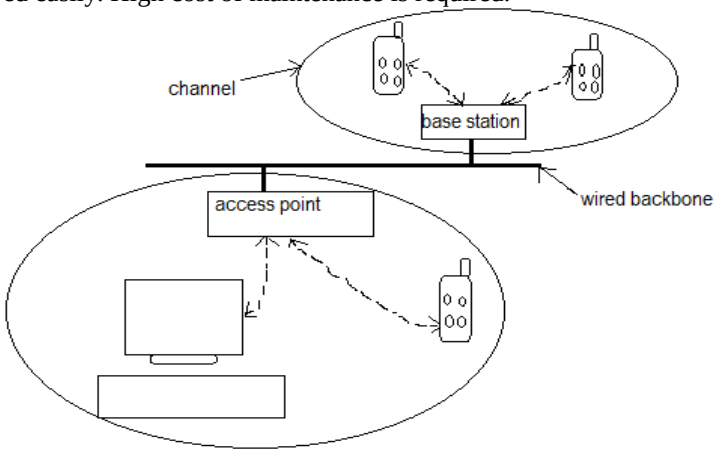

Fig 4: Infrastructured network

B. *Infrastructure-less networks:*

All nodes are mobile and can be arranged in any manner anytime. No dedicated access points, routers etc are needed. It has good speed, convenient in deployment and has relatively low cost. Distributed routing is used mainly. Due to mobility, frequency path breaks. Time synchronization is difficult to achieve. It needs less maintenance then other. Nodes may be heterogeneous or homogeneous.

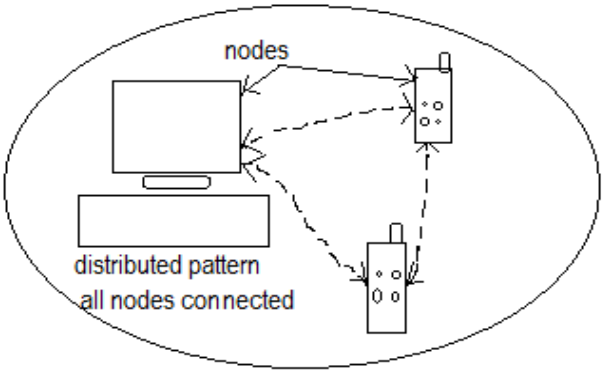

Fig 5: Infrastructure- less network

IV. ATTACKS IN ADHOC NETWORKS

We generally classify the attacks in two types' i.e Active attacks and Passive attacks.

A. *Passive Attacks*:

are the type of attacks which try to get the valuable information from the complete data sent. This attack does not harm the operation. Confidentiality can be violated if the attacker is also able to interpret the data collected. This type of attack is also difficult to find so prevention should be used like encryption mechanisms before sending the data. Snooping is the technique used by attackers which means accessing other user's private information without their authorization. This is very much like eavesdropping but has dissimilarity that it is not limited to gain access to data during transmission. Crackers mostly use this technique for getting passwords, getting conversation etc.

B. *Active attacks*:

mainly disrupt the operation of the protocol and losses some features like availability of data, authentication of users. It also harm nodes by attracting the packets. It has further two types in it i.e External attacks and Internal attacks. Externals attacks are the attacks that can only be implemented by the nodes that are not part of the network. These can be prevented by the standard security measure like very hard encryption, firewalls etc. Internals attacks are done by the nodes which are itself part of the network means only authorized users can carry out this type of attack. This is more difficult to detect than external attacks [1]. There are few parts under these attacks which are discussed below:

a. *Wormhole Attack*:

In the network, a malicious node receives one packet from some location and couples it to other location then packets are send again. The coupling between two attackers is known as worm hole. The link between two attackers can be wired or wireless. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a worm hole even for packets not addressed to itself because of broadcast nature of the radio channel. When wormhole attack occurs properly then it may enhances the position of attackers. [1]

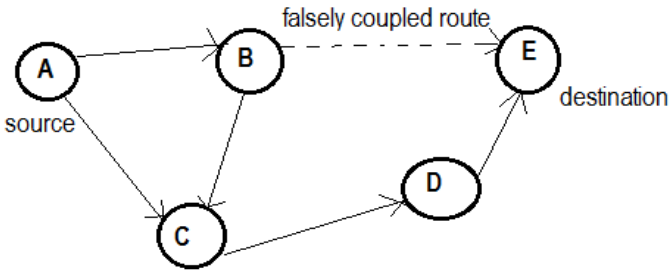

Fig 6. Worm hole attack

In the above figure, A wants to send packet to E. As the packet reaches to the B, B will encapsulate the packet to coupled node E (destination) directly. So the path known to the E is A→B→E. Route discovery done by E will let it be known to the other paths. So the actual route that was followed i.e (A→C→D→E) got encrypted.

b. Black hole attack:

In this, attacker tries to get into the communication network by helping the source to let its packet reaches the desired destination using routing protocols. Attacker gives the shortest path to the destination and it should be suggested before the actual nodes which are part of the network do this job. As the attacker gets into the network, it may damage the packet, modify the packet (confidentiality lost), transmit the packet to another node and it may also drop the packet for doing denial-of-service attack.

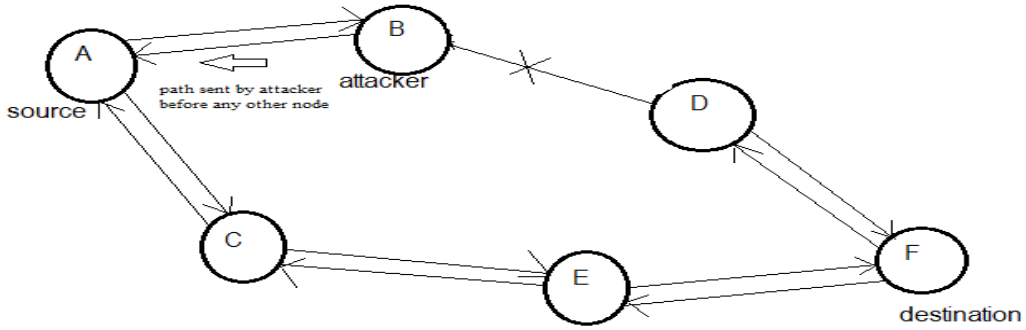

Fig 7. Black hole attack

In the above figure B act like an attacker and will send the shortest path reply before others do. Attacker can then become member of the network and can harm it.

c. Byzantine Attack:

The set of compromised intermediate nodes works together and carries out attacks such as creating routing loops, forwarding packets on irrelevant paths or may dropping packets [2] which makes inconveniency in services. These faults are hard to find. The network seems working properly but shows byzantine behaviour.

d. Revealing Information:

Any type of information stored at any node, it can be secret keys, passwords etc should be kept private or should be protected from any unauthorized access during communication process is going on. An intermediate node can also pass the secret information to any other unauthorized node.

e. *Attack on resources:*

This is a network level attack. An attacker tries to use the resources of other nodes present in network without their permission. Usually targeted nodes are battery power, bandwidth, and computational power, which are present for limited use in ad hoc wireless networks. Attackers send useless requests for different resources and waste the power of resources hired. This also results in sleep deprivation attack which means wasting the power of resources by pumping packets to it again and again.

f. *Replication of packets*:

This is routing attack. An attacker tries to duplicate the useless packets to create disturbances which also results into wastage of battery power resources and bandwidth.

g. Route Cache Poisoning:

In the case of on-demand routing protocols (such as the AODV protocol [4]), route cache (carries route's information) is maintained by each node. This is routing attack

h. *Rushing Attack*:

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [5]. This is routing attack. An attacker receives route request packet from source. Attacker floods the packet rapidly so as to give the shortest path for destination to source before other nodes do this. Source node once gets the reply for shortest path to destination from any node, discard other node's reply. It is also possible that attacker sends the reply for shortest path to source the earliest. Hence, the source node would not be able to find save routes, that is, routes without the attacker. It is extremely difficult to find such attacks in ad hoc wireless networks.

i. *Session Hijacking*:

In this attacker node acts a it is authorized. Every conversation is authorized when session was just built. Attackers takes full advantage of this feature. With the help of spoofing technique used on the IP address of target machine, determines the correct sequence number. Then it performs DOS attack and makes target node unavailable for some time.

j. *Denial of Service*:

This is multi layer attacks. In this, an attacker tries to prevent legitimate and authorized users from the services. That was provided by the network. DOS attack actually relies on the methods or measure that relies on exploiting the network topology. This can be implemented in many ways. Flooding is most common method used in this, so that no other node is able to use the resources on network and will lead to disturb the operation. Malicious node also suggests a poor path so that unnecessarily resources are used again and again and will also take much time to recover. DoS attacks can be generated against any layer in the network protocol stack [6].

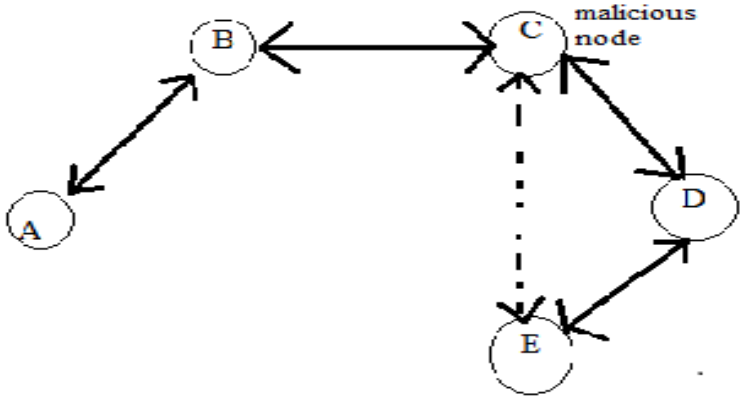

Fig 8. DOS attack

In above figure, C will perform DOS attack. A wants to send packet to E. When packet reaches to C, C will alter the source route as it may delete the node D in route send by A.C will let the E not to listen the route sent by A.

k. Impersonation:

An intermediate node may get access to management system the network of the network and may alter the configurations of the system. An attacker could pretend as an authorized node. It is so mischievous that it may get all the information regarding an authorized node and may also gather all the previous private conversations and harm the whole network. One of the example of this attack is man-in-middle attack.

In the protocol given by Bin Xie and Anup Kumar [7], a defense mechanism is there by which, generation of a valid route discovery message by attacker is not possible and also the anti-authenticating attacked is avoided. But still it cannot avoid some internal attacks like resource consumption attack, black hole attack.

In the protocol given by Ramanarayana & Jacob [8], impersonation, fabrication attacks etc are prevented by secure registration but provide no security from black hole attack, wormhole attack like attacks.

The protocol given by K. Ramanarayana and Lillykutty Jacob [9] prevents modification and fabrication attacks because intermediate nodes authenticate the route via token and is not revealed until the exchange of route request and route reply has finished. This proposed protocol does not avoid collaborative, black hole and gray hole attacks.

In the protocol proposed by Vaidya, Pyun and Nak-Yong Ko [10], mainly modification attacks have been removed.

Altered packets are discarded, and the whole validation is done by intermediate nodes. These protocols provides the security measures for the many of the attacks discussed above but it does not prevent many of the internal attacks.

V. CONCLUSION

We have discussed, the introduction , types, attacks on adhoc networks. Ad hoc network may have wired backbone but is mainly wireless. Ad hoc network can work in a small area only and its speed goes on dividing as the number of nodes goes on increasing. Denial of service also includes misdirection attack. The proposed protocols cannot prevent internal attacks but has very good results in avoiding other attacks. Not only particular alteration of message , dropping packet is prevent but also recognition of attacker can be done.

REFERENCES

1. Hoang Lan Nguyen, Uyen Trang Nguyen. “A study of different types of attacks on multicast in mobile ad hoc networks”. Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008.
2. B. Awerbuch, D. Holmer, C. Nita Rotaru and Herbert Rubens. “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures”. Proceedings of the ACM Workshop on Wireless Security 2002, Pages 21-30, September 2002.
3. C. K. Toh, Chapter 3, “Ad Hoc Wireless Networks”, Prentice Hall, 2002
4. C. E. Perkins and E. M. Royer. "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pages 90-100, February 1999.
5. Y. Hu, A. Perrig, and D. B. Johnson. “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”. Proceedings of the ACM Workshop on Wireless Security 2003, Pages 30-40, September 2003.
6. L. Zhou and Z. J. Haas. “Securing Ad Hoc Networks”. IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999.
7. Bin Xie and Anup Kumar. “A Framework for Internet and Ad hoc Network Security”. IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.
8. Ramanarayana Kandikattu and Lillykutty Jacob. “Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks”. International Journal of Electronics, Circuits and Systems Volume 2, October 2007.
9. K. Ramanarayana, Lillykutty Jacob. “Secure Routing in Integrated Mobile Ad hoc Network (MANET)- Internet”. Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Pages 19-24, 2007.
10. Vaidya, B., Jae-Young Pyun, Sungbum Pan, Nak-Yong Ko. “Secure Framework for Integrated Multipath MANET with Internet**”**. International Symposium on Applications and the Internet, Pages 83 – 88, Aug. 2008.

