Volume 6, Issue 8, August 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review on MANET-Type, Characteristics, Applications and Protocols Used in Blackhole Attacks

Anil
M.Tech Scholar, Department of CSE,
BRCM CET, Bahal,
Haryana, India

Dr. Sudesh Kumar
Asst. Prof., Department of CSE,
BRCM CET, Bahal,
Haryana, India

Abstract— ***Mobile ad- hoc networks(MANETS) are autonomously self-organized networks without infrastructure support. Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network An ad hoc wireless network is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. A variety of routing protocols have been proposed and several of them have been extensively simulated and implemented. This paper gives a brief idea of what is MANET, types, characteristics, applications, mobility model and types of protocols used in blackhole Attacks.***

Keywords— ***MANET, Routing Protocol, Attack, AODV, Blackhole***

I. INTRODUCTION TO MANET

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. These systems work with the support of a centralized supporting structure such as an access point. The wireless users can be connected with the wireless system by the help of these access points, when they roam from one place to the other.The adaptability of wireless systems is limited by the presence of a fixed supporting coordinate. It means that the technology cannot work efficiently in that places where there is no permanent infrastructure. Easy and fast deployment of wireless networks will be expected by the future generation wireless systems. This fast network deployment is not possible with the existing structure of present wireless systems.

Types of Wireless Networks

- Infrastructure based networks
- Infrastructure less (ad hoc) networks

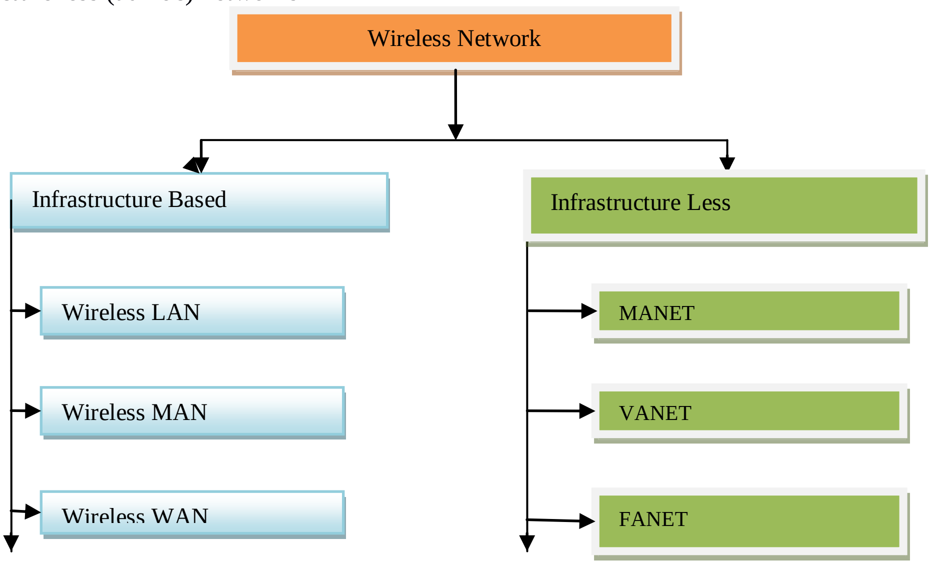

Figure 1 Types of wireless networks

I.I MOBILE AD-HOC NETWORKS (MANET)

A Mobile Ad-hoc network is a collection of the mobile/semi mobile nodes with no pre- established infrastructure forming a temporary network. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared media. Laptop computers and personal digital assistances (PDAs) that communicate directly with each other are some example of nodes in an Ad-Hoc network as shown in figure 2. Nodes in the Ad-Hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi-mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily.

I.II VEHICULAR AD-HOC NETWORKS (VANET)

Vehicular Ad-hoc Networks (VANET) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions and accidents as show in figure 2.

I.III FLYING AD-HOC NETWORKS (FANET)

In FANET nodes UAVs fly in the air without any physical connection. While flying in the air they communicate with each others. So FANET may be defined as a type of infrastructure less networks which is refers to communicate between the flying nodes as show in figure 2.

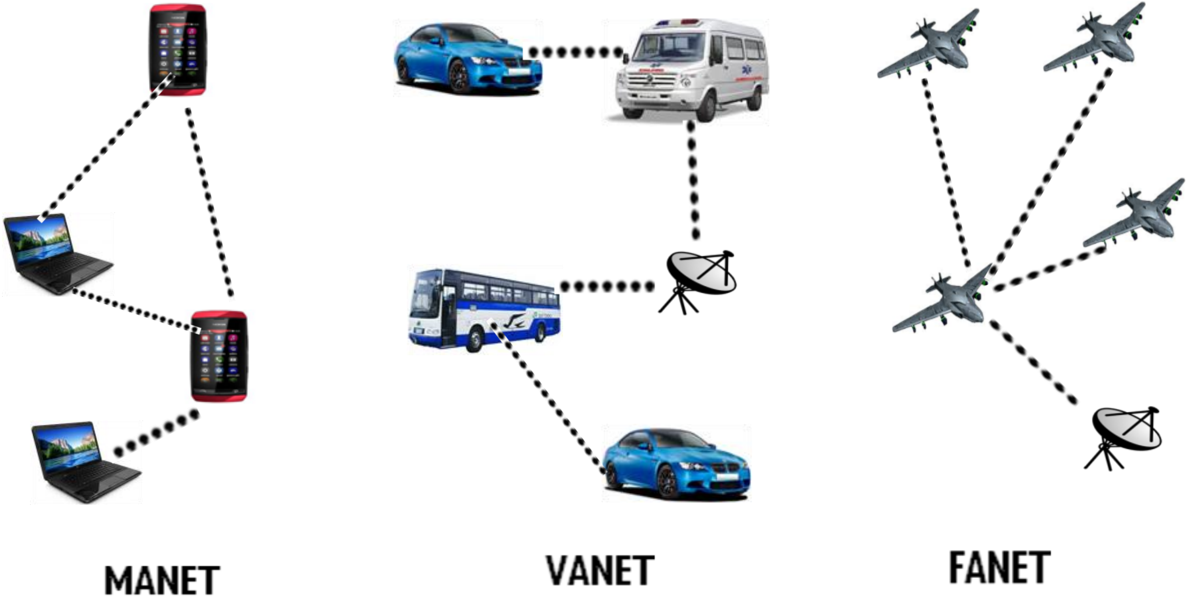

Figure 2: MANET, VANET and FANET

II. CHARACTERISTIC OF MANET

- Autonomous and infrastructure less
- Multi-hop routing
- Dynamic network topology
- Device heterogeneity
- Energy constrained operation
- Bandwidth constrained variable capacity links
- Limited physical security
- Network scalability
- Self-creation, self-organization and self-administration

III. APPLICATION OF AD HOC N/W

- ***Personal uses:-*** in home ,office meeting, smart class in school, n/w at construction sites
- ***Communication :-*** call forwarding ,mobile communication, time dependent services
- ***Business:***- e-commerce , mobile offices , & dynamic database access
- ***Vehicular services***:- road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks
- ***Military battleground:-***
- ***Commercial projects:-***
- ***Education:-*** Universities & college's n/w for communication Smart classrooms for student for better understanding Video calling during meetings or lecture Using net for searching new things relating to study.

IV. MANETS CHALLENGES

1) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
2) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
4) Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
5) Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.
6) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.
7) Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.
8) Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks

V. ROUTING PROTOCOLS

Protocol is a set of rules which are used in networking. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly.

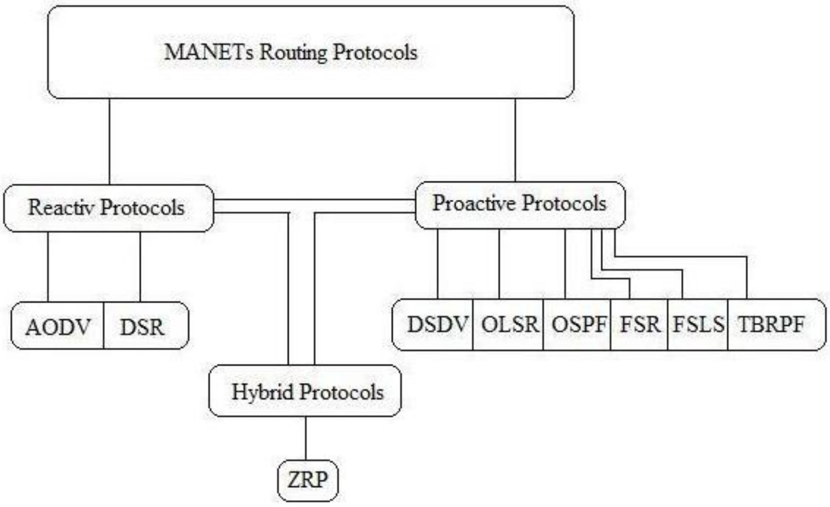

Figure 3. MANET Routing Protocols

A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network [33]. There are many routing protocols in the wireless and ad-hoc environment and all of these protocols are not suitable for the MANET as show in the figure 4.1.

VI. BLACK HOLE ATTACK IN MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). Here describes Black Hole attack and other attacks that are carried out against MANETs.

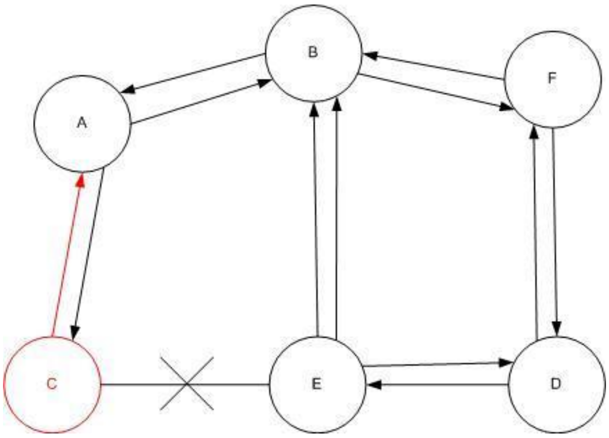

Figure 4. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it . In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address . The method how malicious node fits in the data routes varies. Figure 4 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

VII. INTRODUCTION TO AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV is a reactive protocol, which has same on-demand characteristics with DSR with different maintaining mechanisms of routing table . In AODV, each node stores a routing table, which contains a single record for each destination as show . That is the big difference between AODV and DSR. In DSR each node can store multiple entries in the routing table for each destination. In AODV, the source node (and also other relay nodes) stores the next-hop information corresponding to each data transmission.

- Route Request Message (RREQ):
- Route Reply Message (RREP):
- Route Error Message (RERR):

VIII. PERFORMANCE METRICS

There are following performance matrices to evaluate the performance of the routing protocols.

- Throughput: Throughput or network throughput is the average rate of successful message delivery over a communication channel.
- End-End Delay: The packet end-to-end delay is the time of generation of a packet by the source up to the destination reception. So this is the time that a packet takes to go across the network.
- Packet delivery rate: The total number of data packets received divided by the total number of data packets originated.
- Data Dropped : This is the difference between total number of packet transmitted by transmitter and total number of packet received by receiver at receiver end.
- Network load: The total number of routing messages transmitted divided by the total number of data packets received.

IX. CONCLUSION AND FUTURE SCOPE

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network Infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In our proposed work we analyzed that Black Hole attack with three different scenarios with respect to the performance parameters of End-to-End Delay, Throughput and Packet Delivery Ratio. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols Secure AODV and AODV .The percentage of Packet Delivery Ratio of Secure AODV is better as compare to the AODV. The throughput of Secure AODV is better as compare of AODV. In case of End to End Delay however, there is effect on Secure AODV by the malicious node is similar to the AODV.Based on our research and analysis of simulation result we draw the conclusion that Secure AODV is more vulnerable to Black Hole attack than AODV.For future work several directions are possible. Like by apply Prevention and detection technique of blackhole attack on Secure AODV routing protocol and compare with the existing Secure AODV routing protocol.

REFERENCES

[1] Barleen Shinh, Manwinder Singh, IJECS Volume 3 Issue 12 December, 2014 "A Review Paper on Collaborative Black Hole Attack in MANET"

[2] Aanchal Joshi. "A Review Paper on Black Hole Attack in MANET" International Journal of Advance Research in Computer Science and Management Studies Volume 4, Issue5 ,May2016

[3] Himani Yadav, Rakesh Kumar / (IJERA) Vol. 2, Issue 3, May-Jun 2012" A Review on Black Hole Attack in MANETs"

[4] C.Sivaram murthy, B.S.Manoj, "Adhoc wireless networks: Architectures and protocols", Pearson Education, 2004.

[5] Nai-Wei Lo, Fang-Ling Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET", Intelligent Technologies and Engineering Systems Volume 234 of the series Lecture Notes in Electrical Engineering, 28 February 2013.

[6] Marius Popovici, Daniel Crişan, Zagham Abbas, “wireless network”, The Journal of Mobile Communication, Computation and Information ISSN:1022-0038 (Print)1572-8196, 2015

[7] P. V. Jan i, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 16/17 2002

[8] Aarti, Dr. S. S. Tyagi “Study of MANET: Characteristics, Challenges, Application and Security Attacks” www.ijarcsse.com, Volume 3, Issue 5, May 2013.

[9] Deepa .S, Dr. D.M Kadhar Nawaz,” A Study on the Behavior of MANET Routing Protocols with Varying Densities and Dynamic Mobility Patterns ”, IJCA Special Issue on “Mobile Ad-hoc Networks ”MANETs, 2010

[10] Ashis Bhattercharjee , Subrata Paul (IJETT) –Volume 10 Number 8-Apr 2014”A Review on some aspects of Black Hole Attack in MANET”