Mobile Ad-Hoc Networks: An Overview

Aleburu Deborah .D

ABSTRACT: Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that is formed without the support of any existing network infrastructure. It is a self-configurable network where nodes connect and disconnect from the other nodes in the network automatically at any point in time. The characteristics of MANETs such as flexibility, distributed operation, node to node connectivity make it vulnerable to various security attacks such as wormhole attacks, grey-hole attacks, black-hole attacks and so on. This paper presents an overview of the characteristics, applications, challenges, security goals, limitations, routing protocols and security attacks of MANETs.

Keywords: Mobile Ad-hoc Network, grey-hole attack, flexibility, self-configurable, black-hole attack

1.0 INTRODUCTION

Improvement in technology and wide spread of mobile devices has brought about the demand for new network environment fulfilling individuals requirement for connecting to the internet and networks without limiting time and places; the wireless networks has met this demand. Wireless networks can be classified into two areas; infrastructure network using facilities such as base station and access point, and infrastructure-less network composed with mobile devices. This infrastructure-less networks are referred to as Ad hoc network (Wei-Chen & Horng-Twu, 2015)

Mobile Ad-hoc Network (MANET) is a set of nodes that is created without having the support of any network infrastructure. The MANET is self-configurable network, where nodes connect and disconnect from each other within the network automatically at any time. Flexibility, distributed operation, addressing mobility, node to node connectivity, are some of the characteristics of MANET. Routing of the data in the MANETs are done based on node discovery and then transmission i.e. the node receive the request message and forwards it to neighboring node for further transmission to ensure that its reaches the particular destination and together with the aid of route reply message communication occurs; each node behaves like a relay agent to route the data traffic (Irshad & Shoaib, 2010).

This paper presents an overview on the characteristics, challenges, security goals, routing protocols and security attacks of MANETs. The remaining part of the paper is arranged as follows; section 2 presents the characteristics and application of MANET, section 3 presents the routing protocols in MANET; section 4 discusses the challenges and limitations of MANETs, section 5 presents the security attacks faced by MANETs while section 6 presents the Security goals. Finally, Section 7 gives the conclusion.

2.0 CHARACTERISTICS AND APPLICATION OF MANETS

The following are some of the characteristics of Mobile Ad Hoc Network (MANET) (Aarti & Tyagi, 2013):

1. **Distributed operation:** There is no background network for the central management of the network operations, the management of the network is distributed amongst the nodes. The nodes associated with a MANET cooperate collectively and communicate among themselves and every node behaves as a relay when necessary, to implement specific functions like routing and security.
2. **Multi hop routing:** Any time a node attempts to send information to other nodes which is out of its communication range, the packet is going to be forwarded via a number of intermediate nodes.
3. **Autonomous terminal:** In MANET, each node is a completely independent node that could perform the duties of as both a host as well as a router.
4. **Dynamic topology:** Nodes are able to move willfully with different speeds; thus, the network topology may change randomly as well as at unpredictable time. The nodes in the MANET dynamically establish routing among themselves while they travel around, establishing their unique network.
5. **Light-weight terminals:** In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.
6. **Shared Physical Medium:** The wireless communication medium is available to the entity with the proper equipment and adequate resources. Accordingly, access to the channel is not be restricted.

Some of the typical applications include but not limited to the following (Aarti & Tyagi, 2013):

1. **Military battlefield**: Ad-Hoc networking enables the military to benefit from commonplace network technology to maintain an information network involving the soldiers, vehicles, and military information head quarter.
2. **Collaborative work**: For a lot of business environments, the necessity for collaborative computing is much more important outside office environments than inside and where people must have outside meetings to cooperate and exchange information over a given project.
3. **Local level**: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom.

IJSER

Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

4. **Personal area network and Bluetooth**: A personal area network is a brief range localized network where nodes are often connected with a given person. Short-range MANET for instance Bluetooth can simplify the inter communication between various mobile devices for example a laptop, and a mobile phone.
5. **Commercial Sector**: Ad hoc networks can be utilized in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. (Aarti & Tyagi, 2013).

3.0 ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS (MANETS)

An ad-hoc routing protocol is a standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network (Saxena et al, 2013) . Different protocols are proposed to deal with routing problem in the MANET. The routing protocols in MANET are categorized as:

On Demand Routing or Reactive Routing algorithm: These protocols tend not to retain the routing information in the nodes if they are not the communicating entities. The path calculation is carried out provided that the node wishes to connect to the destination node, for this it broadcasts route request packet to the neighboring node within the network which then further broadcast packet. Once the destination is discovered it sends route reply message using the shortest path. Examples of algorithms in this category include: Ad-hoc on demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing (TORA) (Swati, 2013).

Table driven or Proactive Routing Algorithm: These protocols regularly retain the updated information concerning the nodes in the network. Every node is aware of the other node beforehand which thereby makes the view of whole network within the reach of each and every node. The routing details are retained in the routing tables. Whenever there is a change in the network topology, these tables are also updated. Example of protocols under this category include: Optimized Link State Routing Protocols (OLSR), Destination Sequenced Distance vector routing (DSDV), Cluster Gateway Switch Routing Protocols (CGSR), Fish eye State Routing Protocol (FSR), Wireless Routing Protocol (WRP) (Swati, 2013).

The Hybrid Protocol: The hybrid protocol is one that combines the attributes of both reactive and proactive protocol. Each node maintains routing information about its zone by utilizing the proactive approach. It also uses the reactive approach outside the zone. The challenge of this type of protocol is that the advantage depends on number of other nodes activated and reaction to traffic demand depends on gradient of traffic volume. An example is the Zone Routing Protocol (ZRP) (Nidhi & Yogesh, 2015).

4.0 CHALLENGES AND LIMITATIONS OF MANET

Regardless of the attractive applications, the features of Ad hoc network introduce several challenges that must be studied carefully. These include (Chlamtac *et al*, 2003, HaoYang *et al*, 2004, Ankur *et al*, 2013):

1. **Dynamic topologies**: Since MANET is self-organizing and nodes are liberal to move randomly in the network, the topology changes very frequently and randomly at any point of time. This causes problem in routing the packet to the intended recipient. The position of the node is dynamic so once the route is known it is not certain that the node will still remain for the next couple of minute.
2. **Routing**: Considering that the topology in the network is changing regularly, the challenge of routing packets between any set of nodes becomes a difficult task. Most protocols should be based on reactive routing rather than proactive. Multi cast routing is an additional challenge since the multi cast tree has stopped being static as a result of the random movement of nodes within the network. Routes between nodes might contain multiple hops, which happens to be more technical than the one hop communication.
3. **Device discovery**: Since the discovery of the nodes is monotonous in the distributed environment where movement of the nodes is random, therefore the discovery and existence in the network needs dynamic updates to make possible the selection of optimal route.
4. **Bandwidth-constrained-variable capacity links**: Wireless links will keep having significantly lower capacity than their hardwired counterparts.
5. **Power-constrained and operation**: Some or every one of the nodes within a MANET may depend on batteries or some other exhaustible means for their energy. For these nodes, an important system design criteria for optimization may very well be energy conservation. For the majority of the light-weight mobile terminals, the communication-related functions need to be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.
6. **Security and Reliability**: Beside the common vulnerabilities of wireless connection, an ad-hoc network does have its particular security problems because of issues like nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, as a result of limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission

IJSER

errors. Mobile wireless networks are often prone to physical security threats than are fixed-cable nets. The increased prospect for eavesdropping, spoofing, and denial-of-service attacks needs to be carefully considered.

7. **Quality of Service (QoS)**: Providing different quality of service levels within a regularly changing environment might be a challenge. The inherent stochastic feature of communications quality in a MANET makes it hard to provide fixed guarantees on the services accessible to a device. An adaptive QoS have to be implemented over the traditional resource reservation to support the multimedia services.
8. **Inter-networking**: Besides the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is usually expected in several cases. The coexistence of routing protocols in this mobile device is an issue for the even mobility management.
9. **Diffusion hole problem**: The nodes positioned at the boundaries of holes might be affected from excessive energy consumption because the geographic routing is likely to deliver data packets along the hole boundaries by perimeter routing if it must bypass the hole. This could certainly enlarge the hole due to excessive energy utilization of the boundaries nodes.
10. **Congestion**: When transmission of packets over network is higher than the capacity of network then problem of congestion arises. Packets are dropped and network performance decreases resulting from congestion. Simply congestion means overpopulated. In ad-hoc network overloading of packets can be found at the nodes which could cause loss of packets so data is not successfully delivered at destination.

In MANET the nodes are free to move randomly in the network area. The MANET is self-configurable network, open medium and there are other limitations which make MANET open to various attacks. The reasons are stated below (Swati, 2003):

1. **No Central Authority Control**: As MANET is self-configured network, nodes join and then leave the network when desired. Each node works like a relay agent in forwarding the packets and also the exchange of message is carried with virtually no centralized control. This makes MANET more susceptible to attacks. The node within the network might be a malicious node that is connected with other node as a legitimate user, since there is no mechanism to maintain the system. Without central administration any node can join the network and therefore attack while in the system. In this instance the detection and monitoring of the traffic becomes difficult once the ad-hoc network is large and topology is dynamic.
2. **Availability of Nodes**: As with MANET, communication for the nodes must be available on regular basis in order that the information may be relayed over such path. As nodes are mobile (they are certainly not fixed with any hardware), they are available in various sorts and majority of the nodes depend on the battery. Transmission, reception, routing, retransmission consume power, this is a limitation in MANETs. If in the process of relay of packet the node lost its battery then it will be of no use and the packet transmission will be lost.
3. **Less Secure Boundaries:** MANET network is prone to passive, active attacks and data integrity may be lost because the links are open to numerous security attacks. Attacks are carried out on the link interface, during information exchange involving the nodes and also the link termination between the nodes. The spoofing of one's identity, data tampering, leakage of confidential information, impersonation attacks etc. are some of the harm that is caused by the malicious node.

   Problem of Scalability: In the fixed network the amount of the nodes is known beforehand and also the network topology is created at the initial phase of establishing the network. Since MANET is not fixed, the nodes are mobile and topology changes. The amount of nodes cannot be determined so ad-hoc network needs to be scalable and adaptable to all the new changes it might encounter because of its mobile feature.

5.0 SECURITY ATTACKS IN MANET

The attacks in MANET can be classified based on the source of the attacks i.e. Internal or External, and also based on the behavior of the attack i.e. Passive or Active attack (Irshad and Shoaib, 2010).

1. **External and Internal Attack:** External attackers are mostly away from the networks who wish to gain access to the network and when they gain accessibility into the network they begin sending bogus packets, denial of service in an effort to upset the performance of the whole network. These attacks are similar to the attacks that are carried out against wired network. These attacks can be addressed by implementing security measures such as firewall, where the access of an unauthorized person to the network can be stopped. In internal attack, the attacker desires to have normal access to the network as also take part in the normal activities of the network. The attacker gain access into the network as new node either by compromising an existing node within the network or by malicious impersonation and initiates its malicious behavior. Internal attack is a more severe/dangerous attack as compared to the external attack (Irshad and Shoaib, 2010).

IJSER

2. **Active and Passive Attack:** In an active attack, the attacker disrupts the performance of the network, steal important information and attempt to destroy the information when it is been moved or transmitted within the network (Wei et al, 2007). Active attacks can be an internal or an external attack. The active attacks are designed to disrupt the performance of network; in this case the active attacks behave as an internal node within the network. Being an active part of the network, it is not difficult for the node to use and takeover any internal node to make use of it in introducing bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replay the messages. Attackers in passive attacks usually do not disrupt the normal operations of the network (Wei et al, 2007). In Passive attack, the attacker learns about the network to obtain detail about what is happening within the network. It learns the network in an effort to fully understand the way in which the nodes are communicating with each other, how they can be found in the network. Prior to the attack, the attacker launches an attack against the network, the attacker will need to have enough information regarding the network that it wants to attack so that it can easily hijack and inject attack in the network.

Some of the attacks to MANETs include Black hole, gray hole, flooding, Wormhole, sleep deprivation, jellyfish, modification and so on.

i. **Black Hole Attack**: In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it. In protocol which is 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 (Irshad and Shoaib, 2010).

ii. **Gray Hole Attack**: In this type of attack the attacker tricks the network into agreeing to forward the packets in the network. The moment it obtains the packets from the neighboring node, the attacker drop the packets. This is a form of active attack. Initially, the attacker node behaves normally and replies true RREP messages towards the nodes that sent RREQ messages. Once it receives the packets it starts dropping the packets and initiate Denial of Service (DoS) attack. The malicious behavior of gray hole attack is differs from the others in numerous ways, It drops packets while forwarding them within the network. In other sorts of gray hole attacks the attacker node behaves maliciously for some time till the packets are dropped after which change to their normal behavior (Marti et al, 2008). Due this behavior it is quite challenging for the network to determine such form of attack. Gray hole attack can also be referred to as node misbehaving attack.

iii. **Flooding Attack**: The flooding attack is very easy to implement but cause essentially the most damage. This sort of attack can be carried out through the use of RREQ or Data flooding. In RREQ flooding, the attacker floods the RREQ within the whole network that takes the vast majority of network resources. This may be accomplished by the attacker node by selecting an IP addresses which do not exist in the network. With that no node will be able to reply RREP packets to these flooded RREQ. In data flooding, the attacker enters into the network and set up paths amongst each of the nodes within the network. As soon as the paths are set the attacker injects an enormous number of useless data packets into the network that is forwarded to the rest of the nodes within the network. These unwanted data packets in the network overcrowd the network. Any node that functions as destination node is going to be busy continuously because it is receiving useless and unwanted data at all time.

iv. **Selfish Node**: In MANET the nodes works collectively to be able to forward packets from one node to another node. Any time a node refuses to function in collaboration to transmit packets just to save its limited resources, such nodes are referred to as selfish node, this may cause a major network and traffic disruption (Refaei et al, 2005). The selfish nodes can refuse to forward packets by advertising non existing routes to its neighbor nodes or less optimal routes. The concern of the node is simply to conserve and preserve its resources even though network and traffic disruption would be the side effect of this behavior. The node can utilize the network when it has to make use of it and after utilizing the network it reverse to its silent mode. While in the silent mode the selfish node will not be visible on the network.

v. The selfish node sometimes drop packets, once the selfish node realize that the packets need a large amount of resources, the selfish node stop being interested in the packets, it simply just drop the packets and never forward it in the network.

vi. **Wormhole Attack**: Wormhole attack is a severe attack where two attackers place themselves at strategic locations in the network. The attackers then learns the network, record the wireless data. In wormhole attack, once the attacker gets themselves placed in strategic location in the network, they make the use of their location i.e. they have shortest path between the nodes. They advertise their path to the other nodes in

the network to make them aware that they have the shortest path for the forwarding of their data. The attacker makes a tunnel so as to be able to record any ongoing communication and traffic at one network position and sends them to another position in the network. When the attacker nodes create a direct link between each other in the network, the wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such kind of position the attack is referred to as Out-of-Band wormhole. Another kind of wormhole attack is referred to as In-band wormhole attack; in this type of attack the attacker creates an overlay tunnel over the existing wireless medium. This attack is very much harmful and is the most preferred choice for the attacker (Mahajan et al, 2008).

vii. **Sleep Deprivation Torture Attack**: Another interesting attack in MANETs where the attacker makes sure to keep the nodes awake until all of its energy is lost and the node enter into permanent sleep, this attack is referred to as sleep Deprivation torture attack. The nodes functioning in MANETs have limited resources such as. battery lifespan, the node stays active for transmitting packets throughout the communication. As soon as the communication stops, these nodes resume sleep mode so as to conserve their resources. The attacker capitalize on this aspect of the nodes by making it busy, keeping it awake in an attempt to waste all of its energies making it sleep all through its life. When nodes are asleep permanently an attacker may easily enter into the network and use the remaining portion of the network.

viii. **Jellyfish Attack**: In this type of attack, the attacker attacks the network by introducing unwanted delays inside the network (Nguyen and Nguyen, 2006). In this particular type of attack, the attacker node first get access to the network, once it enter into the network and becomes a part of the network, it then incorporate the delays inside the network by delaying each of the packets that it receives and once delays are propagated then the packets are freed in the network. This allows the attacker to generate high end-to-end delay, high delay jitter and significantly affect the performance of the network.

ix. **Modification Attack:** The main feature of ad-hoc network is the fact that any node can freely join the network and can leave it at any point in time. These way nodes which want to attack the network can also enter the network any time. The malicious node then later takes advantage the irregularities within the network among the nodes. It participates in the communication process and afterwards launches the message modification attack (Wei et al, 2007).

6.0 SECURITY GOALS

All networking functions in MANETs like routing packets as well as forwarding are self-organized and performed by nodes themselves which makes security in mobile ad-hoc networks is a difficult task. The following security goals must be satisfied to evaluate if mobile ad-hoc networks are secure or not (Anuj & Sandeep, 2015):

1) Availability: Availability means that nodes are available or accessible when needed by authorized users. Both data and services come under availability. All network services must ensure availability even when an attack occurs in the network.

2) Confidentiality: Confidentiality ensures that all resources of computer are available only for authorized individuals and accessible by them only. Information exchanged between entities in the network should be protected from un-authorized users.

3) Integrity: Integrity provides a way to access the assets in such a way that only the authorized users can access or modify the information. Information should be original while transferred to the user to ensure Integrity.

4) Authentication: Authentication means that the participants within the network communication are all authorized not fake. The assets of MANETs should be accessed only by authenticated nodes.

5) Authorization: Authorization means assigning various access rights like read, write and both to variant types of participants or users. Let's take an example of network admin that only assigned to perform network management tasks.

6) Flexible to attacks: The network functionalities should be maintained if a number of nodes are lost or compromised.

7) Originality: Originality means newness that ensures about the previously snatched packets does not get retransmitted by the malicious node.

7.0 CONCLUSION

This paper gives an overview of MANET by presenting its characteristics, applications, security goals, limitations and the security attacks. MANETs are being utilized in many fields such as military and disaster response majorly due to their characteristics such as flexibility, mobility, and lack of fixed infrastructure. However, these characteristics make it susceptible to many attacks. In order to protect these systems with limited resources, the security practitioners need to understand the possible security threats and their respective effects on MANET and have a framework to ensure that the protections implemented to mitigate the vulnerabilities in the systems are the most efficient.

REFERENCES

Aarti and Dr. S. S. Tyagi (2013). Study of MANET: Characteristics, Challenges, Application and Security Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering 3*(5), 252-257

Ankur O. B., Prabhakar L. and Ramteke (2013). MANET: History, Challenges and Applications. *International journal of application or innovation in Engineering & Management (IJAIEM).* 2(9), 249-251, ISSN 2319-4847.

Anuj R., Sandeep G. (2015). Review on MANETs Characteristics, Challenges, Application and Security Attacks. *International Journal of Science and Research (IJSR) 4*(2) pp. 2203-2208

Chlamtac I., Conti M., and Liu J. (2003). Mobile ad hoc networking: Imperatives and challenges. Ad Hoc Networks, 1(1), 13–64. doi:10.1016/s1570-8705(03)00013-1

HaoYang, Haiyun and Fan Y. (2004). Security in mobile ad-hoc networks: Challenges and solutions, 11(1), 38-47.

Irshad U. and Shoaib U.R. (2012). Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols. (Master's Thesis)

Marti S., Giuli T.J., Lai K. and Baker M. (2008) Mitigating Routing Misbehavior in Mobile AdHoc Networks.

Mahajan V., Natue M. and Sethi A. (2008). Analysis of Wormhole Intrusion attacks in MANETs. *IEEE Military Communications Conference*, 1-7.

Nguyen H.L. and Nguyen U.T (2006). Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks. International Conference on Networking, Systems, Mobile Communications and Learning Technologies.

Nidhi P. and Yogesh K. (2015). Congestion control mechanism in ADHOC networks: Review. *International journal of Advanced Research in Computer Science and Software Engineering (IJARCCSE), 5*(7), 701-704, ISSN:2277128x.

Refaei M., Srivastava V., Dasilva L. and M.Eltoweissy (2005). A Reputation-Based Mechanism for Isolating Selfish nodes in Ad Hoc Networks. *Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services*, 3-11

Saxena, N., Kumar, S., and Saxena, V. (2013). Performance Analysis of AODV Routing Protocol under the Different Attacks Through The Use Of OPNET Simulator. International Journal of Innovative Research and Development, 2(12), 244–248.

Swati Jain (2013). Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol. Retrieved from https://www.scribd.com/doc/85671348/Final-Dissertation

Wei C., Xiang L., Yuebin B. and Xiaopeng G. (2007). A New Solution for Resisting Gray Hole Attack in Mobile Ad Hoc Networks. *Second International Conference on Communications and Networking in china,* 366-370

Wei-Chen Wu and Horng-Twu Liaw (2015), "A Study on High Secure and Efficient MANET Routing Scheme," Journal of Sensors, vol. 2015, Article ID 365863, 10 pages, 2015. doi:10.1155/2015/365863

IJSER