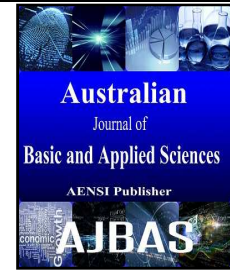




AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com



Security Challenges in Mobile Ad Hoc Networks - A Survey

¹R. Nandakumar and ²K. Nirmala

¹Research Scholar, R & D Centre, Bharathiar University, India

²Associate Professor, Quaid-E-Millath College(W), India.

Address For Correspondence:

R. Nandakumar, Research Scholar, R & D Centre, Bharathiar University, India
E-mail: nandakumar1279@yahoo.com

ARTICLE INFO

Article history:

Received 12 February 2016

Accepted 12 March 2016

Available online 20 March 2016

Keywords:

Challenges, Characteristics, Mobile Ad-hoc Networks, Routing protocols, Security.

ABSTRACT

Mobile ad hoc networks are a kind of temporary networks in which nodes are moving without any fixed infrastructure or centralized administration[1]. Ad-hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. The infrastructure less and the dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies. People and devices are allowed to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments. Routing in Mobile Ad-hoc Networks is a challenging task due to its frequent changes in topologies. We discuss in this paper routing protocol, challenges and security of ad-hoc networks.

INTRODUCTION

Wireless networks consist of a number of nodes which communicate with each other over a wireless channel. There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks. The infrastructure networks, in which mobile devices communicate with base stations that are connected to fixed network infrastructure. Each node in the infrastructure networks is within the range of a fixed access point like base station. Applications of this type include mobile phone and wireless local area networks. The other type of wireless network, infrastructure less networks, is known as **Mobile Ad-hoc Networks (MANET)** (Han, L., 2004). These networks have no fixed access points while every node could be host or router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. These networks are autonomous systems consisting of routers and hosts. These nodes are constrained in power consumption, bandwidth, and computational power (Han, L., 2004). MANETs lack central administration, so the security issues are different and thus requires different security mechanisms than in conventional networks. Wireless links in MANETs make them more prone to attacks. It is easier for hackers to attack these networks easily and thus gain access to confidential information. They can also directly attack the network to delete messages, add malicious messages, or masquerade as a node. This violates the network goals of availability, integrity, confidentiality, authenticity and authorization. MANET require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields during wars, military applications, and other emergency search and rescue situations at the time of disasters. Routing in ad-hoc networks faces additional problems and challenges when compared to routing in traditional wired networks. In this paper, we discuss different routing protocols and challenges of MANETs.

Open Access Journal

Published BY AENSI Publication

© 2016 AENSI Publisher All rights reserved

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

To Cite This Article: R. Nandakumar and K. Nirmala., Security Challenges in Mobile Ad Hoc Networks - A Survey. *Aust. J. Basic & Appl. Sci.*, 10(1): 654-659, 2016

II. Characteristics and Applications:

2.1. Characteristics of MANET:

2.1.1. Autonomous behavior:

In MANET, each node acts as both host and router (Kulkarni, R.V.). It means that a node has ability of host and can also perform switching functions as router so endpoints and switches are indistinguishable.

2.1.2. Multi-hop transmission:

When a source node and destination node for a message is out of the transmission range, the MANETs are capable of multi-hop transmission. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets have to be forwarded through one or more intermediate nodes.

2.1.3. Distributed nature of operation:

As a centralized control is absent here, the control and operation of the network is distributed among the nodes. The nodes should collaborate to implement many functions mainly security and routing.

2.1.4. Dynamically changing topology:

Due to mobile nodes, the change in topology is frequent and dynamic in nature (Kulkarni, R.V.). The connectivity among the nodes may vary with time and dynamically establish routing among them as they move about.

2.1.5. Inferior link capacity:

The reliability, scalability, efficiency and capacity of wireless links are often inferior when compared with wired links. One end to end path can be shared by several sessions. The terminals communicate through which channel is subject to noise, fading, interference and has less bandwidth than a wired network. This shows the fluctuating link bandwidth of wireless links.

2.1.6. Symmetric environment:

All nodes have identical features with similar responsibilities and capabilities. Every node can function as a router or host and hence it forms completely symmetric environment.

2.1.7. Light weight features:

MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.

2.1.8. Absence of Infrastructure:

Ad-hoc networks are supposed to operate independently of any fixed infrastructure.

2.2. Applications of MANET:

2.2.1. Military battlefield:

Military equipment now routinely contains some sort of computer equipment[7]. Through ad-hoc networking, the military could take the advantage of commonplace network technology to maintain an information network among the vehicles, soldiers and military head quarters. Basically the techniques of ad-hoc networks came from this field.

2.2.2. Commercial sector:

Ad hoc can be used in emergency/rescue operations for natural calamities relief efforts, e.g. in fire, flood, or earthquake. Rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is delivered from one rescue team member to another.

2.2.3. Local level:

Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

2.2.4. Personal Area Network (PAN):

Short-range MANET can simplify the intercommunication between various mobile devices (such as a mobile phone, laptops, and wearable computers) (Sun, J.Z., 2001). Traditional wired cables are replaced with

wireless connections. MANET can also extend to access the Internet or other networks by mechanisms e.g. Wireless LAN.

III. Routing Protocols:

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network (Wu, B., 2007). In MANET, there are different types of routing protocols each of them is applied according to the network circumstances. The basic classification of the routing protocols in MANETs are,

3.1. Proactive Routing Protocols:

Proactive routing protocols are also called as table driven routing protocols. In this each node maintain routing table which contains information about the network topology even without requiring it. The routing tables are updated periodically whenever the network topology changes (Mohammed, E.). Proactive protocols are not appropriate for large networks as they need to maintain node entries for each and every node in the routing table of every node. There are various proactive routing protocols. Example: DSDV, OLSR, WRP etc.

3.2. Reactive Routing Protocols:

Reactive routing protocol is also known as on demand routing protocol. In this type of protocol, route is discovered whenever it is needed. Nodes initiate route discovery when demanded. A route is acquired by the initiation of a route discovery process by the source node. This routing protocol have two major components:

3.2.1. Route discovery:

In this phase source node initiates route discovery on demand basis. Source nodes consults its route cache for the available route from source to destination otherwise if the route is not present it initiates route discovery. The packet of the source node includes the address of the destination node as well address of the intermediate nodes to the destination.

3.2.2. Route maintenance:

Due to dynamic topology of the network cases of the route failure between the nodes arises due to link breakage etc, so route maintenance is required. Reactive protocols have acknowledgement mechanism due to which route maintenance is possible. There are various reactive routing protocols. Example: DSR, AODV, TORA and LMR.

3.3. Hybrid Routing Protocol:

This type of protocol is a trade-off between proactive and reactive protocols. Proactive protocols have more overhead and less latency while reactive protocols have less overhead and more latency (Wu, B., 2007). Thus a Hybrid protocol is needed to overcome the shortcomings of both proactive and reactive routing protocols. This protocol is a combination of both proactive and reactive routing protocol. It uses the on demand mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Hybrid protocol is appropriate for large networks where large numbers of nodes are present. In this, large network is divided into a set of zones where routing inside the zone is done by using proactive approach and outside the zone routing is done using reactive approach. There are various hybrid routing protocols for MANET like ZRP, SHRP etc.

IV. Challenges:

Regardless of many characteristics, the MANET introduces several challenges that must be studied carefully. These are following:

4.1. Routing:

Due to the constantly changing topology in ad-hoc networks, routing the packets between any pair of nodes becomes a challenging task. Most of the protocols based on reactive routing instead of proactive routing. Multi cast routing is another challenge as the multi cast tree is not static due to the random movement of nodes within the network. Routes between the nodes may have multiple hops, which is more complex than the single hop communication.

4.2. Security and Reliability:

Ad hoc networks have security problems e.g. nasty neighbour relaying packets (Frodigh, M., 2000). The feature of distributed operation requires different schemes of authentication. Further, wireless link features also introduce reliability problems, because of the limited transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility induced packet losses, and data transmission errors.

4.3. Quality of Service:

Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic characteristic of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive Quality of Service must be implemented over the traditional resource reservation to support the multimedia services.

4.4. Inter-networking:

In addition to the communication within an ad hoc network, inter-networking between MANET and infrastructure networks (mainly IP based) is often expected in many cases. The routing protocols coexistence in such a mobile device is a challenge for mobility management.

4.5. Power Consumption:

For most of the light-weight mobile devices, the communication-related functions should be optimized for lean power consumption. Power conservation and power-aware routing must be considered.

4.6. Multicast:

Multicast is desirable to support multiparty wireless communications (Chlamtac, I., 2003). As the multicast tree is not static, the routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

V. Security:

We discuss security criteria and attacks which are following:

5.1. Security Criteria:

5.1.1. Availability:

The term Availability means that a node should maintain its ability to provide all the designed services regardless of its security state. This security criterion is violated mainly during the denial-of-service attacks, in which nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable.

5.1.2. Confidentiality:

Means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that are not authorized to access them (Goyal, P., 2011).

5.1.3. Integrity:

Message being transmitted is never corrupted. Integrity can be compromised mainly in two ways (Li, W., A. Joshi, 2008): Malicious altering, Accidental altering. When the message is removed, repeated by an attacker with malicious goal, it is called as malicious altering; on the other hand, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

5.1.4. Authentication:

Ensures that participants in communication are genuine and not impersonators. It is necessary for the communication entities to prove their identities as what they have claimed using some techniques. If there is not such an authentication mechanism, the attacker could act as a benign node and thus get access to confidential information, or even insert some fake messages to disturb the normal network operations.

5.1.5. Non-repudiation:

Ensures that the sender and the receiver of a message cannot deny that they have ever sent or received a message (Garg, N., R.P. Mahapatra, 2009). This is useful when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that it has received an erroneous message, it can then use that message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

5.1.6. Authorization:

No one else can pretend to be another authorized member to learn any useful information. It is generally used to assign different access rights to different level of users.

5.1.7. Attacks using fabrication:

Generation of false routing messages is termed as fabrication. Such types of attacks are difficult to detect.

5.2. Attacks on Manet:

There are various kinds of attacks on ad hoc network which are following:

5.2.1. Location Disclosure:

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. By using traffic analysis techniques, simpler probing and monitoring approaches, an attacker is able to detect the location of a node, or the structure of the whole network.

5.2.2. Black Hole:

In a black hole attack a malicious node injects false route replies to the route requests, announcing it as having the shortest path to a destination (Lundberg, J., 2000). These fake replies can be fabricated to divert network traffic through the malicious node for simply to attract all traffic towards it in order to perform a denial of service attack by discarding the received packets.

5.2.3. Replay:

A replay attack is one of the attacks that degrade severely the performance of MANET. A replay attacker does this attack by interception and retransmission of the valid signed messages. The validation of signed messages is verified by a timestamp discrepancy fixed by sender and receiver nodes. This attack usually attack on the freshness of routes (Singh, K., 2009).

5.2.4. Wormhole:

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network. The connection between the nodes that have established routes over the wormhole link is completely under the control of the two conspiring attackers. The packet leashes is the solution to this attack.

5.2.5. Blackmail:

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the attacker. An attacker may construct such reporting messages and try to isolate legitimate nodes from the network. The non-repudiation security criteria can prove to be useful in such cases since it binds a node to the messages it generated.

5.2.6. Denial of Service:

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legal routes.

5.2.7. Routing Table Poisoning:

Routing protocols maintain tables that hold information regarding routes of the network. In this type of attacks, the malicious nodes generate and send fabricated signalling traffic, or modify legitimate messages from other nodes, in order to add false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can have non-optimal routes, routing loops, bottlenecks, and even portioning certain parts of the network (Lundberg, J., 2000).

5.2.8. Breaking the neighbour relationship:

An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.

5.2.9. Masquerading:

During the neighbour acquisition process, an outside intruder could masquerade a nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

5.2.10. Impersonation:

Impersonation attack is a severe threat to the security of mobile ad hoc network. As we can see, if there is not such a proper authentication mechanism among the nodes, the attacker can capture some nodes in the network and make them look like friendly nodes. Thus, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

5.2.11. Eavesdropping:

It is another kind of attack that usually happens in the mobile ad hoc networks. Eavesdropping means to obtain some confidential information that should be kept secret during the communication. The confidential information may include the public key, private key, location and passwords of the nodes. Because such data are very confidential to the nodes, they should be kept secret so that unauthorized nodes can't access this.

VI. Conclusion:

Mobile ad hoc networking is one of the most important and essential technologies that support future computing scheme. The characteristics of MANET bring this technology as a great opportunity together with many challenges. Nowadays, MANET is becoming an interesting research topic and there are many research projects employed by academic and companies all over the world. MANETs can be exploited in a wide area of applications like military, battlefields, emergency search and rescue, law enforcement, commercial, local and personal contexts.

REFERENCES

- Patil, M. J., M.P. Deshmukh, 2015. A Review Paper on Introduction of Parallel Manipulator and Control System. In International Journal of Engineering Research and Technology (Vol. 4, No. 02 (February-2015)). ESRSA Publications.
- Han, L., 2004. Wireless Ad-hoc Networks.
- Frodigh, M., P. Johansson, P. Larsson, 2000. Wireless ad hoc networking: the art of networking without a network. Ericsson Review, 4(4): 249.
- Wu, B., J. Wu, E.B. Fernandez, M. Ilyas, S. Magliveras, 2007. Secure and efficient key management in mobile ad hoc networks. Journal of Network and Computer Applications, 30(3): 937-954.
- Li, W., A. Joshi, 2008. Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.
- Singh, K., R.S. Yadav, A. Ranvijay, 2009. A review paper on ad hoc network security. International Journal of Computer Science and Security, 1(1): 52.
- Sun, J.Z., 2001. Mobile ad hoc networking: an essential technology for pervasive computing. In Info-tech and Info-net. Proceedings. ICII 2001-Beijing. International Conferences on , 3: 316-321. IEEE.
- Chlamtac, I., M. Conti, J.J.N. Liu, 2003. Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1): 13-64.
- Kulkarni, R.V., A. Shelke, R. Gaikwad, P. Kawade, Energy Consumption Using Sleep And Awake Mechanism In Manets.
- Goyal, P., V. Parmar, R. Rishi, 2011. Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11: 32-37.
- Garg, N., R.P. Mahapatra, 2009. Manet security issues. IJCSNS, 9(8): 241.
- Mohammed, E., L. Dargin, Routing Protocols Security in Ad Hoc Networks. Oakland University School of Computer Science and Engineering CSE, 681.
- Lundberg, J., 2000. Routing security in ad hoc networks. Helsinki University of Technology, <http://citeseer.nj.nec.com/400961.html>.
- Rai, A.K., R.R. Tewari, S.K. Upadhyay, 2010. Different types of attacks on integrated MANET-Internet communication. International Journal of Computer Science and Security, 4(3): 265-274.