International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A Review on Mobile Ad hoc Networks (MANETs)

P. Kalaiselvi MCA., M.Phil.,
Asst. Prof in M.Com (CA),
Sri Vasavi College (SFW)
Mail Id: kalai.pmsk@gmail.com
Ph: 8883846635

ABSTRACT- A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. The security is a major issue and the chances of having the vulnerabilities are also more. In this paper we discuss various types of vulnerabilities, attacks and security goals in MANETs.

1. INTRODUCTION:

An ad-hoc network is formed when more stations come together to form an independent network. Ad-hoc networks do not require any prior infrastructure; therefore, they are also termed as infrastructure-less networks consisting of both fixed node and mobile nodes exchange data with each other without any centralized infrastructure or base station. The transitional node behaves like router to transmit data to nodes not in range. Each node in the MANET having its own processing capability and energy resources and the mobile nodes are moving rapidly. MANET can be easily established in any emergency situations which can be used in disaster recovery, conferences, emergency situation in hospitals, meetings, lectures. Mobile Ad-hoc network has a number of protocols which are classified as reactive, proactive and hybrid for difference types of MANET such as AODV, DSR, OLSR, TORA and GRP.

Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1 and node 2. The

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

node 2 will act as a router and these three nodes together form an ad-hoc network.

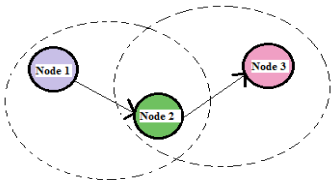

Fig 1: Example of mobile ad-hoc network

2. MANETS CHARACTERISTICS

2.1. Distributed operation: There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves.

2.2. Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

2.3. Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time.

2.4. Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

2.5. Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

3. ADVANTAGES OF MANETS

The advantages of an Ad-Hoc network include the following:

- They provide access to information and services regardless of geographic position.
- Independence from central network administration.
- Self-configuring network, nodes are also act a routers.
- Less expensive as compared to wired network.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

- Scalable—accommodates the addition of more nodes.
- Improved Flexibility.
- Robust due to decentralize administration.
- The network can be set up at any place and time.

4. MANET VULNERABILITIES

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

4.1 Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc Network. Lack of centralized management will impede trust management for nodes.

4.2 Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures.

4.3 Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4.4 Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

4.5 Dynamic topology: Dynamic topology and changeable nodes membership may

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

5. ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network. There are a number of attacks that affect MANET. These attacks can be classified into two types:

5.1. External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

5.2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious that is part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

5.2.1. Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

5.2.2. Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

key, private key, password etc. can be fetched by eavesdropper.

5.2.3. Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

5.2.4. Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

5.2.5. Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray-hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

6. SECURITY GOALS:

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

6.1 Availability: A node should maintain its ability in order to provide all the designed services.

6.2 Integrity: It guarantees the identity of messages sent when they are sent. Integrity may be altered by activity of malicious node or accidental altering by node.

6.3 Confidentiality: Information access is possible only for authorized node.(ie) Confidentiality will be maintained in accessing messages by the way of providing privileges to authorized nodes.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

6.4 Authenticity: Providing assurance for the nodes which are participating in the communication and not the impersonators.

6.5 Non-Repudiation: It ensures that the sender cannot deny or repudiate that he has not send the message and receiver cannot deny or repudiate that he has not receive the message.

CONCLUSION:

Mobile Ad hoc Network is a flexible and adaptive network with no fixed infrastructure. Nowadays, MANET is used in crisis management and military operations. Security is a critical issue in the field of computer networks. They are more vulnerable to attacks and we have improved the quality and issues in Mobile Ad-hoc network. In this paper we have described about infrastructure, characteristics and advantages of MANE. And also we have described about vulnerabilities, attacks and security goals in MANETs.

REFERENCES:

1. P.Visalakshi, S.Anjugam "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey" International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005 National Conference on Architecture, Software system and Green Computing.
2. R.Maheswari, S.Rajeswari "A Review on Types of Jamming Attack In Mobile Ad-Hoc Network" Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications,27th March 2015 Special Issue .
3. Aashish Mangla, Vandana "Detection of Physical Jamming Attacks in MANETs" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015.
4. Sachin Lalar "Security in MANET: Vulnerabilities, Attacks & Solutions" International Journal of Multidisciplinary and Current Research General Article ISSN: 2321-3124 Available at: http://ijmcr.com.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-168 PAGE NO: 1024-1030
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

5. Baljiinder Singh, Dinesh Kumar "Jamming attack in MANET: A Selected Review" International Journal of Advanced Research in Computer Science and Software Engineering 5(4), April- 2015, pp. 1264-1267.

All Rights Reserved ©2017 International Journal of Computer Science (IJCS Journal) &
Department of Computer Science, Sri Vasavi College, Erode, Self-Finance Wing, Erode, Tamil Nadu, INDIA
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals
http://www.skrgcpublication.org/