

A Review on Challenges Faced by Manets

Mrs. Annie Jose
Lecture, Govt Polytechnic College
Vechoochira, Pathanamthitta
Kerala, India

Abstract— Mobile Adhoc Networks (MANETs) are the emerging technology in the field of local area wireless communications. These are network of mobile nodes spontaneously built without any predefined infrastructure with self routing and data communication. The special features of these networks in turn make the design of this network a more challenging task. The self configuring nature of the network also poses several security issues. This paper is focusing on the challenges faced by MANETs.

Keywords— MANETs, Security, Challenges

I. INTRODUCTION

A group of independent nodes that are free to move in and out of the network come together to work in a self centered manner to achieve a common goal of data communication from one point to another within the network form a MANET [1]. The highly autonomous nature of these networks will make them more prone to attacks. These networks are self routing type without central station, so each node in the network has to act as router also. The nodes in the network are having diverse architecture with different security policies. MANETs are need to be implemented with at most care otherwise it will lead to big security failures. Like any other wireless networks, MANETs are also at high risk of attacks from passive and active attackers in the system or from outside the system [2]. The general architecture of mobile ad-hoc network is shown in figure 1.

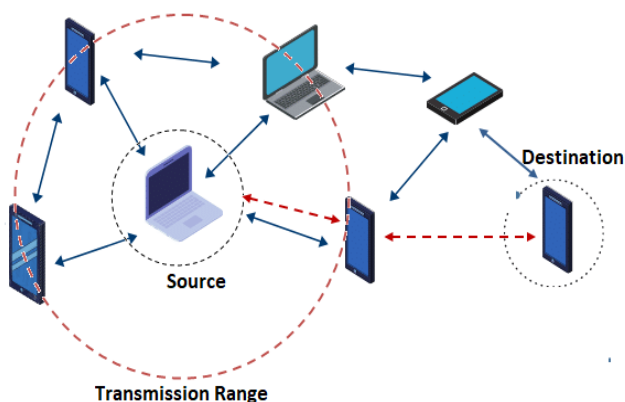


Fig 1: Mobile Ad-hoc networks

The tremendous increase in the number of portable wireless devices are also contributing for the enhanced importance in wireless communications. This type of devices are very fast in mutual communication in the given communication area. So this makes the fast setup of mobile networks using any of the available devices in emergency situations. Hence these

networks are mainly used in critical and emergency situations like rescue operations and military applications.

II. CHALLENGES FACED BY MANETS

MANETs have many advantages when compared to the existing wired networks the speed, ease to set up, lack of predefined infrastructure and central station are some of them. Self-configuration and self-routing are also make MANETs unique. These characteristics of MANETs pose many challenges. The routing is a process that each node has to do in MANETs, so routing protocols used in these networks are different from the protocols of the wired networks [3]. Unlike wired networks protocols the security issues are not taken care by the routing protocols developed for these networks. All these together raise certain challenges in these networks.

Resource constraints: the nodes in the network are autonomous so they should have sufficient computational facilities, memory requirements and power resources. The nodes in the network are heterogeneous in nature and may not be doing a single dedicated task. The processing capability, memory requirement and power sources are the responsibility of individual nodes. So a route change or link break in the network can result due to the limitations of the resources. Many more factors like bandwidth availability, transmission range, interference from multiple devices, etc are also some of the issues to be addressed by the researchers to make these networks more efficient[4].

Changing topology: nodes in MANETs by definition itself are free to move within or out of the network and cause frequent location change, link breaks, and hence packet loss. This is one of the major challenges faced by MANETs. As the node mobility increases transmission impediments can occur [5]. This can lead to other problems like hidden or exposed nodes, interferences, fading etc.

Routing: Lack of centralized routing facilities like routers and gateways in MANETs forces each node in ad-hoc networks to act as routers. The protocols for MANETs are five layered and is similar to Transmission Control protocol/Internet Protocol (TCP/IP). As each node is initiating and identifying suitable route for communication, it has to do all the processes like route identification, addressing, data encapsulation and de-capsulation by itself. The dynamic topology of MANETs makes the routing process a difficult task. The protocols designed for MANETs include both reactive and proactive types. Both are having their own advantages and disadvantages in terms of efficiency and resources requirements.

Security: In any communication system data security includes confidentiality, integrity, availability and non-

repudiation. Unlike the wired routing protocols the protocols of wireless networks are not ensuring data security. So the data communication is prone to attacks. Multi-hop routing and lack of boundaries add to the security issues. The routing processes in these networks need mutual trust which can be reason for malicious node to become a part of the network without getting noticed. The attacks can be passive or active. A passive attack violates the confidentiality rights of the nodes and the data collected by malicious nodes may be used for future active attacks. The different protocol layers are affected by different attacks. Packet dropping, data modification, substitution, false routing are some of the physical layer active attacks. Denial of service, masquerade attack, replay attack, selective forwarding, node replication, wormhole attack, sinkhole attack, Sybil attack etc. are more severe active attacks in wireless networks [6].

The various challenges faced by the mobile ad-hoc networks are summarized in the table 1.

Table 1: Challenges in MANETs

Challenges	Parameters	Factors affected
Resource constraints	Memory requirement	Need more storage space to support routing and security
	Processing power	Mismatch between system speed and service provider, Non uniform capabilities of nodes
	Power consumption	Battery life is a major concern of mobile nodes.
	Bandwidth	Open medium, limited bandwidth
	Antenna	Unreliability of wireless medium, Transmission errors
Topology	Node mobility	Connectivity and packet loss Unpredictability of environment
	Link break	Routing and packet loss, Loop formation
Routing	No routers or central station	Complex routing process Link error, packet loss, Hidden / exposed nodes
Security	Passive attacks	Mainly affect physical layer
	Active attacks	All layers are affected

III. CONCLUSION

Ubiquitous nature of MANETs makes them suitable to set up networks in all situations instantaneously. As they are a collection of nodes without predefined infrastructure the system has much vulnerability. Based on the literature review, the major concerns in the system can be categorized into four major areas: the resources, network topology, routing and security. All these factors affect the performance of the network in one-way or the other.

REFERENCES

- [1] Sana Fatima, Mrs Suma R, 2015, Security Challenges in MANETs and the Solution to Overcome Them, International journal of engineering research & technology (ijert) icesmart – 2015 (Volume 3 – Issue 19)
- [2] Shibu, K. R., & Pramila, R. S. (2021). Load Based Key Generation for MANETs: A Comparative Study with DSR and AODV. *Wireless Personal Communications*, 116(3), 1703-1712.
- [3] Ms. Monika Kashap, Mr. Sukhvir Singh, Ms. Rimpay Kumari, 2013, Routing Issues and Challenges for manets: a review, international journal of engineering research & technology (ijert) Volume 02, Issue 10 (October 2013)
- [4] Shibu, K. R., & Sujipramila, R. (2021). Secret Key Generation by Exploiting Traffic Load for Mobile Adhoc Networks. *Wireless Personal Communications*, 1-14.
- [5] Shibu, K. R., & Pramila, R. S. (2021). Load Based Key Generation for MANETs: A Comparative Study with DSR and AODV. *Wireless Personal Communications*, 116(3), 1703-1712.
- [6] Shibu, K. R., & SujiPramila, R. (2018). Routing protocol based key management schemes in manet: a survey. *International Journal of Engineering & Technology*, 7(3), 1453-1456.