Energy efficiency in MANET: A review

Priyanka*, Mr. Sandeep Goel**

**Research Scholar, Department Of Electronics And Communication Engineering, Master of Technology In Electronics & Communication Engineering, Guru Jambheshwar University Of Science & Technology, Hisar (Haryana)*

***Assistant Prof. (ECE), Department Of Electronics And Communication Engineering, Master of Technology In Electronics & Communication Engineering, Guru Jambheshwar University Of Science & Technology, Hisar (Haryana)*

Abstract - Ad hoc is the network which is considered as a composition of various types of devices that are communicating with one other directly. Several Ad hoc networks are considered as local area networks in which computers and different other devices have been enabled to transfer data in direct way to one another instead of transferring through a centralized access point. Usually Ad hoc network does not need any router and any wireless base station. This network is established for single session only. Administrator could set multiple hop Ad hoc networks that could be used for the transmission of information on multiple nodes. It is created to solve specific problem. It becomes permanent network if someone is going to establish such network for longer period. The Wireless networks are getting popularity since 1970. In several decades a lot of researches have been developed on Ad hoc Network. The most vital role in case of martial applications is played by ad hoc networks & many researches like global mobile information program.

Keywords: Wireless networks, information, Administrator, Network, MANETs, etc.

I. INTRODUCTION

Nowadays, most organizations and companies make their services available on the Internet so that they may be reached by many different users. In contrast, if multiple users ask for a service, it is better to use multicast transmission in order to save time and effort. By using the broadcast nature of wireless transmission, a multicast can be used to improve the efficiency of a network by sending a number of copies instead of sending one copy individually; this may reduce the communications cost of applications that use multicast instead of unicast. A great number of current applications require a reliable multicast scheme, meaning that one sender must ensure data delivery to multiple receivers; this may sometimes be hard to do, especially in a wireless environment. Wireless environments may suffer from packet loss more frequently than wired environments, but such losses still happen in both environments. By using multicast transmission, we can reduce the consumption of links' bandwidth and reduce the time for using these links.

A mobile ad hoc network is a combination of moving mobile nodes that form a temporary network without support from any centralized admission or infrastructure such as access points or base stations. The term ad hoc is of Latin origin and means "for this purpose," which in this case signifies that the network exists for special circumstances and is dismantled easily (on-the-spot).

In MANETs, all moving nodes coordinate among themselves to enable communication and to manage routing and resources; this is done in a distributed manner. This means that each node in the MANET must be more intelligent, so that it can operate as a sender for transmitting messages, can receive data from another master sender that received the original message, and can work as a router for forwarding packets to other nodes.

MANETs work in a highly dynamic and distributed nature, and nodes are mostly battery powered and have a limited power source; thus, energy consumption is a key issue in MANETs, sometimes causing failures in a node that can affect the whole network. If one node runs out of power, the probability of network separation will increase; therefore, to prolong the lifetime of the MANET, we need to consider energy efficient ways to reduce the consumption of network energy, such as announcing the remaining energy of a node, which will avoid depletion of energy and reduce the probability of network separation.

Ad hoc Network (Mobile):

Ad hoc Network (Mobile) has been considered as wireless Ad hoc network. It has been considered as a continuous self-configuring, without infrastructure network of the mobile devices which are linked wirelessly mobile. The network which works as the composition of various types of devices is Ad hoc network. These devices are communicating to one other in direct way. Several Ad hoc networks are considered as local area networks in which computers and different other devices have been enabled to transfer data in direct way to one another instead of transferring through a centralized access point. In case of mobile Ad- hoc network does not need any router. It does not need any wireless base station. This network is established for single session only. If someone wants to share file in multiple computers then he

could set more than one hop Ad hoc network that can be used to transfer information on more than one node. It is created to solve specific problem. It becomes permanent network if someone is going to establish such network for longer period.

The Wireless networks are getting popularity since 1970. In several decades a lot of researches have been developed on Ad hoc Network (Mobile). Ad hoc Network (Mobile) based networks has been performing an important role in case of martial applications & many researches like global mobile information program. This is useful in case of programs that are related to near digital radio. There can be new spaces of industrial & commercial applications for those networks which are based on wireless Ad hoc. The fast development of internet has made communication a useful factor for Computation. In recent era of mobile devices usually we stay online. It is compulsory to make network cost effective & very fast to stay online all time.

Wireless Networks:

The network that uses wireless data connections is known as wireless network. These connections have been used to connect nodes of network. Wireless networking is the method. The costly process of including cables may be avoided through using this methodology by telecommunications networks and enterprise installations. Wireless network have been managed using radio communication. Such implementation is taking place at physical layer.

Security Issues in Ad hoc Network:

MANET has been exposed to various attacks because of lack of central authority. There are several resource constraints also. Third party has provided data & infrastructure management. In case of Ad hoc network protection of Network has big concern. It has been risky to provide sensitive information to service provider of Ad hoc Network. Protection breach may result in customer or business loss. Thus vendors have provided security to the accounts. This section discusses the different type of attack on routing. There are two types of attack on routing that are passive attack and active attack. The passive attack is further classified as Eavesdropping and Routing Information hiding. A passive attack generally checks data which has been not converted traffic & would checks for sensitive information & clear-text passwords which could be utilized in different variety of attacks. Passive attacks comprise of analysis of traffic, decrypting on weekly basis encrypted traffic, monitoring of unprotected communications & capturing validated information as passwords that user enter to login. In case of Eavesdropping there is unauthentic real-time interception of transmission. The examples are phone call, fax transmission, instant message or videoconference. Eavesdrop came into existence from practice of standing.

Advantages of MANETs

Here some advantages of MANETs are given as:

- The first advantage is Sovereignty from central network administration.
- It has the facility of self-configuring, nodes are also routers
- It provide us self-healing through continuous re-configuration
- It is scalable: accommodates the addition of more nodes

Disadvantages of MANETs:

Here some disadvantages of MANETs are given as:

- Limit of physical and security resources.
- Inherent joint trust susceptible to attacks
- Scarcity of the facilities of authorization.
- Detection of malicious node has been made hard by unstable topology of network.
- Security protocols cannot work for Ad hoc networks as it work for wired networks

II. MANET MULTICASTING: CHALLENGES AND ISSUES

Issues and challenges presented by MANET multicasting include the following.

Resource Management:

Mobile nodes in MANETs are limited in resources such as power and memory, so a multicast protocol minimizes the consumption of these resources and utilizes them in such a manner as to ensure competent handling of information with efficient resource consumption, such as by minimizing the use of state information packets.

Link Failure:

Because of the random mobility of the nodes and the wireless nature of links, link stability is hard to preserve in mobile ad hoc networks.

Control Overhead:

In multicast transmission, we need to keep track of the members involved in the multicast transmission; thus, we need control packets to be exchanged between them. Since only limited bandwidth is provided in MANETs, this may result in significant overhead requirements, so the design of MANET should take into consideration the need to keep the control packet size to a minimum.

Efficiency:

In MANETs, errors and failure are more likely to happen than in ordinary networks due to their mobility and limited bandwidth. Therefore, in the multicast protocol design, efficiency is very important. Efficiency as used here is the ratio of received data to the total number of transmitted packets in the network.

Reliability:

Reliability is the key issue in multicast transmissions in MANETs, and this can be difficult to deliver due to the differentiation in the members involved and the fact that any member can disconnect from the network at any time, in consideration of its environmental conditions.

Wireless Nature:

The wireless nature of a MANET makes it vulnerable to the numerous types of attacks that are common to wireless links such as snooping, interference, and eavesdropping, which may also affect the network resources. Attackers can use these methods to prevent the normal communication scenario among nodes or to capture valuable information.

No Defined Physical Boundary:

Due to mobility, we cannot define exactly the boundaries of our network, and the nodes can join or leave the network because of radio coverage. The scalability of MANETs is changing, so the security mechanism must be able to handle large networks as well as smaller networks, which makes for a difficult task.

Absence of Centralized Management:

Detection of possible attacks is difficult due to the absence of centralized management such as an access point or base station that can monitor the traffic in a MANET, especially if the network is deployed over a large scale, which may delay the trust between involved nodes.

Infrastructure:

Mobile ad hoc networks are infrastructure less, and there is no central administration that can regulate the communication between involved nodes. This means that every node can communicate with other nodes, which makes it difficult to detect faults happening in the network, and because of the highly dynamic topology of MANET, frequent network separation and route changing can result in the loss of packets.

Limitation in Power:

The nodes in mobile ad hoc networks are battery powered; this restriction may cause problems such as the loss of packets, or the nodes may work in a selfish manner, meaning that they do not forward messages received.

Trust

The lack of central administration and the highly dynamic topology of MANETs may result in a lack of trust between involved nodes due to the absence of verification and the fact that some nodes may participate in a transmission even if they are not part of the network, which may result in security breaches in the network or leaks of valued information.

Security:

Attacks may happen in MANETs due to their wireless nature and the lack of centralized admission of mobile ad hoc networks, which make these networks vulnerable to attacks such as eavesdropping and wormhole or black hole attacks. As such, it is essential for the multicast protocol to ensure security.

Quality of Service:

The applications that currently rely on MANETs vary greatly, and these include military applications. Quality of service is an important issue in such applications, but ensuring quality of service by multicast can be difficult for reasons including throughput, delay, and reliability. The design of a multicast protocol should take into consideration the need to provide these parameters.

III. CONCLUSION

Ad hoc networks have been considered as wireless networking paradigm for mobile hosts for particular purpose only. While old mobile wireless networks rely on fixed infrastructure, Ad hoc networks are independent. It is very necessary to stay online all the time in today's society because of development of mobile devices. For staying online 24 x 7 there is an issue for fast connectivity and cost effectiveness while moving among various infrastructures, Ad hoc networks are dealing with these type of problems. Secondly, we discussed security criteria for mobile Ad hoc networks and presented main attack types they are prone to. After the development of Ad hoc network, mobility of the nodes that connect network is possible. In that case a military squad is in attack and need to get away, the nodes would be capable of moving freely in Ad hoc networks. The information would be routed through new paths if old paths are broken. These types of networks are capable of handling clusters.

IV. REFERENCES

[1] Amandeep Kaur, Dr. Amardeep Singh (2014) A Review on Security Attacks in Mobile Ad hoc Networks, International Journal of Science & Research, Volume 3 Issue 5, May 2014, PP. 112-125

[2] Kshitij Bhargava, "Packet dropping attacks in MANET: a survey Journal of Advanced Computing & Communication Technologies" (ISSN: 2347 - 2804) Volume No.2 Issue No. 3, June 2014, PP. 108-119

[3] Lucas Leão explained Flbra: "Fuzzy Logic Based Routing Algorithm For Indoor Wireless Sensor Networks" Network Global Journal of Computer Science & Technology" Volume 11 Issue 4 Version 1.0 might 2014, PP. 567 587

[4] Maulik H. Davda, "A Review Paper Need of infrastructure less, Securing Mobile Ad hoc Networks Against Packet Dropping Attack" Network Global Journal of Computer Science & Technology" Volume 11 Issue 8 Version 1.0 might 2014, 108-119

[5] Md. Waliullah, (2014) "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014, PP. 251-256

[6] P. Kiruthika Devi, Dr. R. Manavalan(2014) "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5 No. 09 Sep 2014, PP. 879-895

[7] Priyanka Rawat, Jean Marie Bonnin, "Wireless sensor network has emerged as one of most promising technologies for future" Network Global Journal of Computer Science & Technology" Volume 05 Issue 7 Version 1.0 might 2014, PP. 134 -146

[8] Sangeeta Yadav (2014) "Hybrid TCP/IP & UDP: A Review Article" International Journal of Advanced Research in Computer Science & Software Engineering, Volume 4, Issue 5, May 2014, PP. 56-68

[9] Zainab Hassan.: "Performance Analysis of Dynamic Wireless Sensor Networks using Linguistic Fuzzy" Advanced Engineering Informatics, sVol.27, No.1, pp. 108-119, 2014