ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 3; May-June-2017; Page No. 93-96

Survey on Routing Protocols for MANETs based on Mobility

D Venkatesh[1], A Subramanyam[2]

[1]Research Scholar, PP. COMP. SCI & ENG. 0459, Department of Computer Science and Engineering,

Rayalaseema University, KURNOOL – 518 007, A.P, India

dvvenkatesh@yahoo.co.in

[2]Professor & Dean of Engineering, Department of Computer Science and Engineering,

Annamacharya Institute of Technology and Sciences, Rajampet, Kadapa, Andhra Pradesh, India

smarige@gmail.com

Received 14 April 2017; Accepted 14 May 2017

ABSTRACT

Topology-Based routing protocols become no longer appropriate for MANETs when the nodes are relatively mobile due to the immoderate overhead of keeping up-to date network topology records. Now a day's cluster based and geographic based routing algorithms are notably studied due to the fact of availability of diverse positioning services for example the global positioning device (GPS). Geographic routing is a promising technique for huge-scale wi - fi ad hoc networks because of its simplicity and scalability. Since direction control procedure isn't always required in geographic routing, it includes a less overhead compared to different routing schemes, like topology based routing protocols. In this research paper we are aiming to analyze the performance of diverse geographic and cluster based routing protocols in mobile ad hoc networks.

Keywords: Global Positioning System, MANET, Ad Hoc Networks, Topology

INTRODUCTION

A wireless network is that which transmits data in packets from computer to computer. Instead of using a central base station (access point) to which all computers must communicate, this peer-to-peer mode of operation can greatly extend the distance of the wireless network and so are susceptible to the wireless network attacks [2]. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. MANET is a particular type of Wireless Mesh Network (WMN). A MANET is a collection of mobile users that communicate using wireless links. In MANET, nodes are mobile and energy constrained.

Issues in Ad Hoc Networks

- Bandwidth Constraints
- Frequent Topology changes
- Limited Battery powers

The selecting the particular routing protocol is based on the process shown in figure 1.

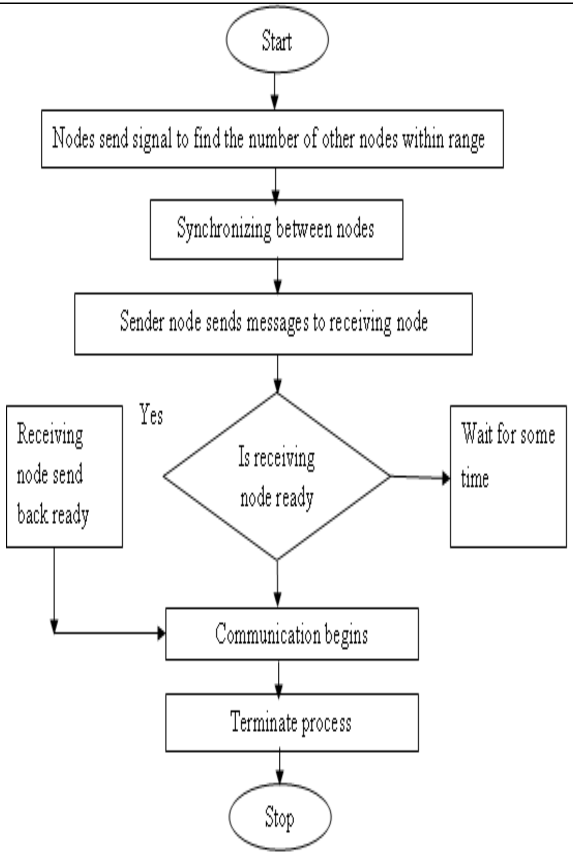
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node sends messages to receiving node
Yes
Receiving node send back ready
Is receiving node ready
Wait for some time
Communication begins
Terminate process
Stop

Figure 1: Working of general Ad Hoc Network

**Corresponding author: D Venkatesh |*

In a traditional wired network no of node connected does not change frequently so its scale is generally predefined but in ad hoc network nodes are mobile numbers of nodes connected in network changes frequently so its scale keeps on changing frequently. As a results its protocols and services such as key management, routing protocols should be compatible to this change [3]. MANET works without the support of a particular device to form communication and therefore gained lot of importance. It is configured and operated without any centralized authority. The participating nodes that are present in this network themselves act as routers and forward the packets in the specified path. Once the source and destination is identified, the node transfers data to other nodes present in the network directly that are present in its transmission range. The nodes that are present in between source and destination will act as intermediate nodes and will be used to forward the data to the nodes that are not in transmission range. This type of network is also called as multi hop Ad Hoc network because the source node will take the help of intermediate nodes to forward the data to the destination node

Challenges of MANETs

The challenges that we are going to face when we use the MANETs are listed below:

➢ Possessing the communication path energizing with fewer complexes and more consistent.

➢ Highly dynamic topology

➢ Network availability

➢ Determination of reliable and stable paths for achieving consistency throughout the communication.

➢ Mobility of the nodes.

➢ Boundaries on mobile nodes

➢ Packet drop in the course of communication

➢ Restrictions of the physical layer

➢ Limitation of Battery life

➢ Network security

Applications of MANETs

There are many applications of Mobile Ad Hoc Networks. These applications of MANETs differ from small static to large scale, mobile and highly spirited networks.

Some well known applications are listed below:

➢ Military operations: For speed and possibly short term formation of military communication and group deployment in combative situations.

➢ Search and Rescue operations: For communication in areas with little or no wireless infrastructure

➢ Disaster relief operations: For communication in environments where the existing infrastructure is damaged or not able to implement fixed infrastructure.

➢ Law enforcement: For secure and fast communication during law and administration operations.

➢ Commercial use: For enabling communications in exhibitions, symposiums and conclave

Security in MANETs

Security is essential service for MANETs because all network services are configured on – the – fly. When the security of a given MANET architecture is not properly designed from the beginning, it is difficult to achieve security goals in practical networks during the network deployment.

To secure a MANET one usually considers the objectives confidentiality, availability, integrity, authenticity and non repudiation. Confidentiality ensures that secret information in the network is never revealed to unauthorized nodes. i.e. the assurance that data is not disclosed to unauthorized parties. Availability ensures that the requested network services, such as bandwidth and connectivity, are available in a timely manner and service is not denied to authorize users. i.e. the assurance that data is readily accessible. Integrity ensures that message or packet being transferred between nodes is not altered or corrupted. i.e. the assurance that data is genuine. Authentication ensures the correct identity of the peer node it is communicating with. Non-repudiation ensures that the originator of a message cannot falsely deny having sent the message. i.e. the assurance that a node cannot later deny the data was sent by it.

Node mobility in a MANET poses many security problems and vulnerable to different types of security attacks than conventional wired and wireless networks due to their open medium, dynamic network topology, absence of central administration, distributed cooperation, constrained capability, and lack of clear line of defense. The unconstrained nature of a wireless medium of MANETs allows the attackers for interception, injection, and interference of communication. Without proper security, mobile hosts are easily captured, compromised and hijacked by malicious nodes. Malicious nodes behavior may deliberately disrupt the network so that the whole network will be suffering from packet losses. Damages include leaking secret information, message contamination and node impersonation.

Before MANETs are successfully deployed, security issues must be addressed. Usually, cryptographic techniques are used for secure communications in wired and wireless networks. The method of using security solutions of traditional wired networks is not suitable for providing security in MANETs. The main problem of any public-key based security system is to make each user's public key available to others in such a way that its authenticity is verifiable. Conventional security solutions to provide public key management is implemented with public key infrastructure (PKI), in which a trusted third party (TTP) holds the public key certificates of all participating entities and acts as an online certification authority (CA) to provide a public key verification service. MANETs do not provide on-line access to trusted authorities or to centralized servers. Implementing public key management and certificate distribution is more challenging due to the - problematic key exchange, session handling, absence of any infrastructure and centralized services, frequent node mobility, wireless link instability, possible network partitions, and configuration of all network services on-the-fly. For these reasons, traditional security solutions that require on-line trusted authorities or certificate repositories are not well suited for securing MANETs. Use of public key cryptography and certificates is one of the effective ways of securing a MANET.

The main security problems that need to be dealt with in MANETs are: the secure storage of key/data in the devices; the authentication of devices that wish to communicate to each other; the secure key establishment of a session key among authenticated devices; and the secure routing in multi-hop networks [1].

MANET ROUTING PROTOCOLS

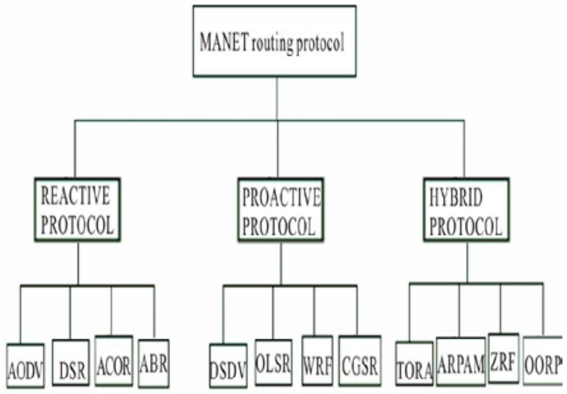

Figure 2: Categories of Routing Protocols

Mobility causes the building and cracking of connection regularly in an indefinite manner. Movable instruments are currently minute, moveable, and extremely incorporated. The usage of routing protocols is to impetuously communicate data through complete network paths employed to reach the destination and prefer the optimal path to arrive at the sink network. Routing protocols are involved in defining the directions safeguard a set of recommendations that permit a number of objects to communicate with one another. The nodes participating in carrying the packets on MANET are not aware of the framework.

Therefore routing algorithms recognizes the structure by procuring the broadcast information from its corresponding nodes and riposte accordingly. The routing protocols are grouped depending on the distinct routing techniques. The necessities of routing protocols are lower path achievement delay, rapid path reconfiguration, loop – free routing, distributed routing method, less control overhead, able to expand, QoS provisioning, assistance for time – sensitive traffic, security and privileged. The ad hoc path consists of source, sink, and in – between nodes. The movement by any of these nodes disturbs the rationality of the path.

CONCLUSIONS

MANETs have acquired increasing research interest in latest years. There are many research projects involved with MANETs. Mobile ad hoc networks are wi-fi networks that use multi-hop routing in place of static networks infrastructure to offer network connectivity. MANETs have applications in unexpectedly deployed and dynamic military and civilian systems. The network topology in MANETs normally modifications with time. Therefore, there are new demanding situations for routing protocols in MANETs seeing that traditional routing protocols won't be appropriate for MANETs. This study is a strive in the direction of a comparative study of generally used mobile ad hoc routing protocols (DSR[4], AODV[5] and TORA[6]). Over the beyond few years, new requirements have been introduced to beautify the abilities of ad hoc routing protocols. As a result, ad hoc networking has been receiving an awful lot attention from the wi-fi studies network. We can summarize our final conclusion as: Increase inside the density of nodes yields to an increase within the suggest End-to-End delay. Increase inside the pause time results in a decrease in the suggest End-to-End delay. Increase within the quantity of nodes will cause boom inside the mean time for loop detection.

REFERENCES

1. Perkins, C.E.: Ad Hoc Networking. Addison Wesley (2001)
2. Mehran Abolhasan, Tadeusz Wysocki, and rykDutkiewicz. A review of routingprotocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia,2003.
3. Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.
4. Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Technical report, Nokia Research Center; University of California, Santa Barbara; University of Cincinnati, November 2001. draft-ieftaodv- 09.txt –
5. David B. Johnson, Yih-Chun Hu, David A. Maltz, Jorjeta G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). [6] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks