ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Survey of Wireless Adhoc Network for MANET

K. Prabu*
Asst Professor,
Dept of Computer Applications,
SRASC, Chidambaram, Tamilnadu, India.
kprabu.phd@gmail.com

Dr. A. Subramani
Prof & Head / MCA,
KSRCE, Thiruchengode,
Namakkal, Tamilnadu, India.
subramani.appavu@gmail.com

Abstract — In the recent year Mobile Adhoc Networks [MANET] have been widely researched for many years. Mobile Adhoc Networks are a collection of two or more devices equipped with wireless communication and networking capabilities without infrastructure. The majority of applications are in areas where rapid deployment and dynamic reconfiguration are necessary and a wire link network is not available. The node should deploy an intermediate node to be the router to route the packet from the source toward the destination. The Mobile Adhoc Network do not have gateway because every node can act as the gateway. The traditional protocol such as TCP/IP has limited use in Mobile Adhoc Networks because of the lack of mobility and resources. In this paper survey on the current status and direction of research on Mobile Adhoc Network.

Keywords: — Adhoc Networks, MANET, Routing Protocols, Energy Efficient, Security.

I. INTRODUCTION

Technology has advanced by leaps and bounds in the last few years. This is evident from the recent developments in various fields such as Medicine, Computer science and Information technology. In no other field has these developments been more evident than in field of wireless technology. Though wireless systems have existed since the 1980's it is only in recent times that wireless systems have started to make inroads into all aspects of human life. Mobile Ad Hoc Networks (MANETs) are advanced wireless communication networks. Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless links. Each node operates as an end system and a router for all other nodes in the network. A mobile Ad hoc Network is a self configuring network of mobile routers connected by wireless links. In 1970 U.S. started a research project to interconnect the tactical units deployed in areas of military conflict without requiring the presence of a fixed network. The project, called PRNET (Packet Radio Network), used a combination of ALOHA and CSMA protocols, combined with a Distance Vector Algorithm. In 1980 Evolved into SURAN (Survivable Adaptive Radio Network), uses hierarchical routing protocol Link State Algorithm. In 1990 IETF created MANET working group, looking for standardizing the relevant aspects of adhoc networks to use in commercial applications. In 2000 was created the Ad Hoc Network Consortium in Japan, aiming to unite the interests and efforts of industry. In 2010 Nowadays, it is using in many projects, especially where we cannot have a fixed infrastructure [1][2][3]. Mobile networks can be classified into **Infrastructure** networks and **Infrastructureless** network

The **Infrastructure** networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone. This type of network can be shown as in fig.1.

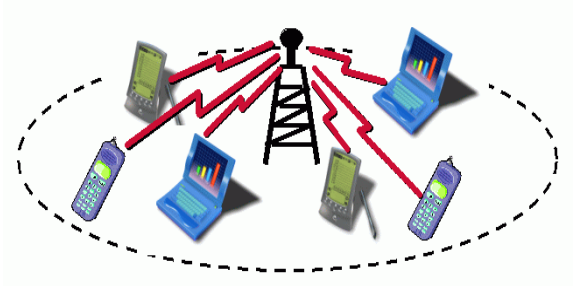

Figure.1. Infrastructure Network.

The **infrastructureless** networks, is knows as Mobile Ad-hoc Networks (MANET). These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move freely. In this type of networks can be show fig. 2.

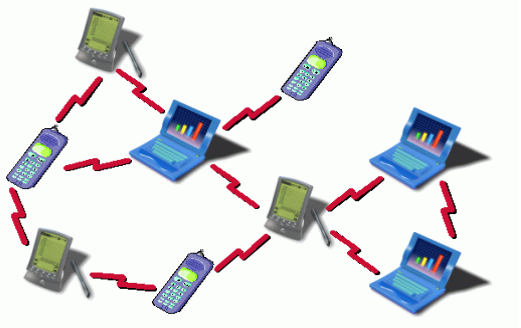

Figure.2. Infrastructureless Network

II. ROUTING PROTOCOLS IN MANET

Routing is the Exchange of information (in this case typical term 'packets') from one station of the network to the other. The major goals of routing are to find and

maintain routes between nodes in a dynamic topology with possibly uni-directional links, using minimum resources. A protocol is a set of standard or rules to exchange data between two devices. These protocols find a route for packet delivery and deliver the packet to the correct destination. Routing protocols are classified into unicast, multicast and broadcast routing protocols. Unicast forwarding means a one-to-one communication, i.e., one source transmits data packets to a single destination. Multicast routing protocols come into play when a node needs to send the same message to multiple destinations. Broadcast is the basic mode of operation over a wireless channel; each message transmitted on a wireless channel is generally received by all neighbors located within one-hop from the sender. The studies on various aspects of unicast routing protocols have been an active area of research for many years such as **Table Driven or proactive, On-Demand Driven or reactive and hybrid routing protocols** [4][15][16][17]**.** This type of protocol can be show as in fig.3.

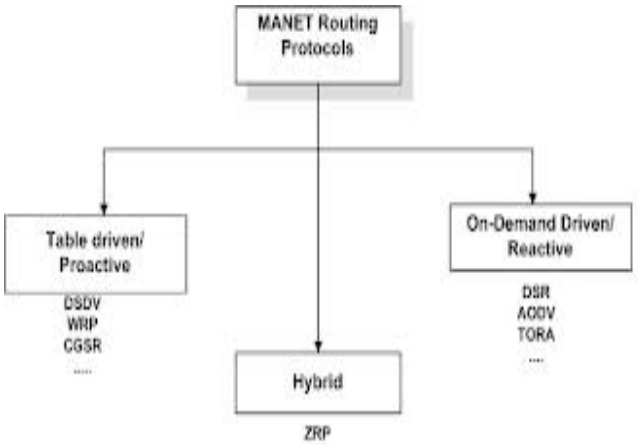

Figure.3. MANET Routing Protocols

Table Driven or Proactive Protocols: keep track of routes for all destinations in the ad hoc network are called Proactive protocols or Table-driven Protocols, as the routes can be assumed to exist in the form of tables. Each node maintains one or more tables containing routing information to every other node in the network. All nodes keep on updating these tables to maintain latest view of the network. The main advantage is that Communications with arbitrary destinations experience minimal initial delay from the point of view of the application. The Disadvantages of proactive protocols is that Additional control traffic is needed to continually update stale route entries. In Table Driven routing protocols some of the existing table driven or proactive protocols are:

i) **DSDV (Destination sequenced distance vector).**
ii) **CGSR (Cluster-head gateway Switch routing).**
iii) **WRP (Wireless routing protocol).**
iv) **STAR (Source tree adaptive routing protocol).**
v) **OLSR (Optimized link state routing protocol).**
vi) **FSR (Fisheye state routing protocol).**
vii) **HSR (Hierarchical state routing protocol).**
viii) **GSR (Global state routing protocol).**

On Demand or Reactive Protocols: In these protocols, routes are created as and when required [5]. When a transmission occurs from source to destination, it invokes the route discovery procedure. The route remains valid till destination is achieved or until the route is no longer needed. The Advantage is that due to the high uncertainty in the position of the nodes, however, the reactive protocols are much suited and perform better for ad-hoc networks. The Disadvantages of reactive protocols include High latency time in route finding and excessive flooding leading to network clogging. Some of the On Demand or Reactive Routing Protocols are:

i) **DSR (Dynamic source routing).**
ii) **AODV (Ad hoc on-demand distance vector).**
iii) **ABR (Associative based routing).**
iv) **SSA (Signal stability based adaptive routing).**
v) **PLBR (Preferred link based routing protocol).**
vi) **TORA (Temporally ordered routing).**
vii) **FORB (ipv6 flow handoff in adhoc wireless network).**

Hybrid Routing Protocol: This protocol is belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned or within a particular geographical region are said to be within the routing zone of the given node. For routing within this zone a table-driven approach is used. For nodes that are located beyond this zone an on-demand approach is used. Disadvantages of hybrid protocols is that success depends on amount of nodes activated and Reaction to traffic demand depends on gradient of traffic volume. Some of the Hybrid Routing Protocols are:

i) **CEDAR(Core extraction distributed adhoc routing).**
ii) **ZRP (Zone Routing Protocol).**
iii) **ZHLS(Zone based hierarchical link state routing).**

III. RESEARCH CHALLENGES IN MANET

The main challenges in mobile ad-hoc networks are as follows:

a) **Limited Bandwidth**
b) **Quality-of-Service**
c) **Energy Efficient**
d) **Dynamically Changing Topology**
e) **Security**
f) **Mobility-induced route changes**
g) **Mobility-induced packet losses**
h) **Battery constraints**

In Mobile Ad-hoc networks have to suffer many challenges at the time of routing. Dynamically changing topology and no centralized infrastructure are the biggest challenges in the designing of a Mobile Ad-hoc network. The position of the nodes in an Ad-hoc network continuously varies due to which we can't say that any particular protocol will give the best performance in each and every case topology varies very frequently so we have to select a protocol which dynamically adapts the situation. Another challenge in MANET is limited bandwidth. If we compare it to the wired network then wireless network has less and more varying bandwidth. So, bandwidth efficiency is also a major concern in ad-hoc network routing protocol

designing because sometimes data has to be transmitted within real time constraints. Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

A Mobile Ad-hoc Network (MANET) is composed of mobile nodes without any infrastructure. MANET applications such as audio/video conferencing, webcasting requires very stringent and inflexible Quality of Service (QoS). The provision of QoS guarantees is much more challenging in MANETs than wired networks due to node mobility, limited power supply and a lack of centralized control. Many researchers have been done so as to provide QoS assurances by designing various MANET protocols. QoS provision will lead to an increase in computational and communicational cost. In other words, it requires more time to setup a connection and maintains more state information per connection. The improvement in network utilization counterbalances the increase in state information and the associated complexity and various issues are needed to be faced while providing QoS for MANET [6][7][8].

The major problems that are faced are as follows:

i) Unreliable channel: The bit errors are the main problem which arises because of the unreliable wireless channels. These channels cause high bit error rate and this is due to high interference, thermal noise, multipath fading effects and so on. This leads to low packet delivery ratio.

ii) Maintenance of route: The established routing paths may be broken even during the process of data transfer. Hence the need for maintenance and reconstruction of routing paths with minimal overhead and delay causes. The QoS aware routing would require the reservation of resources at the intermediate nodes. The reservation maintenance with the changes in topology becomes cumbersome.

iii) Mobility of the node: Since the nodes considered here are mobile nodes, that is they move independently and randomly at any direction and speed, the topology information has to be updated frequently and accordingly so as to provide routing to reach the final destination which result in again less packet delivery ratio.

iv) Limited power supply: The mobile nodes are generally constrained by limited power supply compared to nodes in the wired networks. Providing QoS consumes more power due to overhead from the mobile nodes which may drain the node's power quickly.

v) Lack of centralized control: The members of any ad hoc networks can join or leave the network dynamically and the network is set up spontaneously. So there may not be any provision of centralized control on the nodes which leads to increased algorithm's overhead and complexity, as QoS state information must be disseminated efficiently.

vi) Channel contention: Nodes in a MANET must communicate with each other on a common channel so as to provide the network topology.

vii) Security: Security can be considered as a QoS attribute. Without adequate security, unauthorized accesses and usages may violate the QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposures. The physical medium of communication is inherently insecure.

IV. RESEARCH ISSUES IN MANET

Some issues in mobile ad-hoc networks are as follows:

A. ENERGY EFFICIENT
B. SECURITY

A. ENERGY EFFICIENT*:* Limited power supply is the biggest challenge of an ad-hoc network so if we want to increase the network lifetime (duration of time when the first node of the network runs out of energy) as well the node lifetime then we must have an energy efficient protocol. So an ad-hoc routing protocol must meet all these challenges to give the average performance in every case [12][13][14].

A wireless network interface can be in one of the following four states: **Transmit Receive, Idle** or **Sleep.** Each state represents a different level of energy consumption. **Transmit:** A node is transmitting a frame with some transmission power. **Receive:** A node is receiving a frame with some reception power. That energy is consumed even if the frame is discarded by the node because it was intended for another destination, or it was not correctly decoded **Idle (listening):** Even when no messages are being transmitted over the medium, the nodes stay idle and keep listening the medium. **Sleep:** when the radio is turned off and the node is not capable of detecting signals, no communication is possible. The node uses the power that is largely smaller than any other power.

Energy aware metrics the majority of energy efficient routing protocols for MANET try to reduce energy consumption by means of an energy efficient routing metric, used in routing table computation instead of the minimum-hop metric there are four possibilities to save power from the devices:

i) Minimal Energy Consumption Per Packet: The energy consumption is the sum of power consumed on every hop in the path from a packet. The power consumption on a hop is a function of the distance between the neighbor and the load of this hop. So it is interesting to choose a route where the distance between the nodes isn't too long and also it is interesting to take a shorter route so there aren't too many hopes on the route where the power level gets down.

ii) Maximize Network Connectivity: This metric tries to balance the load on all the nodes in the network. This assumes significance in environment where the network connectivity is to be ensured.

iii) Minimum Variance in Node Power Levels: This metric proposes to distribute the load among all nodes so that the power consumption remains uniform to all nodes. This problem is very complex when the rate and size of data packets vary. When every node has the same level in power, you can be sure that the network functions longer. Because when there is a node which has to switch off because of the power level the whole network is in danger and it can break down the connectivity between the nodes.

iv) Minimize Maximum Node Cost: This metric minimizes the maximum cost per nodes for a packet after routing a number of packets or after a specific period. So a node can be blocked for routing to save battery power. This metrics saves the connectivity from every node. When a node has been used several times for route, it blocks itself to save the power.

B. SECURITY*:* The role of this section is to provide the main goals and challenges which characterized the routing protocol of MANET. Security includes the following goals [9][10][11]:

i) Confidentiality: 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 do not have the privilege to access them.

ii) Availability: Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel.

iii) Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

iv) Integrity: Guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

v) Non-repudiation*:* Ensures that the origin of a message cannot deny having sent the message. Nonrepudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

Attacks in MANET:

In general, the attacks on routing protocols can generally be classified as routing disruption attacks and resource consumption attacks. In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or 175 selfish nodes may try to inject false packets in order to consume network bandwidth.

Classification of the possible attacks in MANET.

a) Impersonation Attack: 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 adversary can capture some nodes in the network and make them look like benign nodes. In this way, 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.

b) Modification Attack: In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes.

c) Flooding attack: attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

d) Black hole attack: A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

V. CONCLUSION

In the recent time there has been a lot of interest in the field of wireless networks. The fast moving world demands seamless communication facilities, so former types of connectivity like wired networks, radio waves are fast becoming obsolete. One of the recent developments in the world of wireless technology is the use of Mobile Ad hoc Networks are an ideal technology which was initially developed for military applications. The rapid use of MANET has resulted in the identification of several problems. In all, although the widespread deployment of Mobil ad hoc networks is still years away, the research in this field will continue being very active and imaginative. In this paper present survey of MANET and its issues and challenges in bandwidth allocation, dynamically changing topology, security issues and energy efficient.

VI. REFERENCES

[1]. C.E. Perkins, "Ad hoc Networking", Addison Wesley 2001.

[2]. C.K. Toh, "Adhoc Mobile Wireless Networks: Protocols and Systems", Printice Hall, New Jersy, 2002.

[3]. C. Siva Ram Murthy and B.S. Manoj "Adhoc Wireless Networks Architectures and Protocols" Prentice Hall 2004.

[4]. Abolhasam, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile adhoc networks. AdHoc Networks, 2(1), 1-22.

[5]. Perkins, C.E., & Royer, E.M. (1991). Adhoc on-demand distance vector routing. Proceedings of the 2nd IEEE (WMCSA) (pp.90-100).

[6]. Zeinalipour-yazeti demetrios "A glance at quality of service in Mobile Ad-hoc networks" final research report for CS 120- Seminar in Mobile Ad-hoc networks, Fall 2001

[7]. Philipp Becker "QoS Routing Protocols for Mobile Ad-hoc Networks – A Survey" August 2007

[8]. Z. J. Haas, J.Deng, B. Liang, P.Papadimitratos and S. Sajama, "Wireless Ad-Hoc Networks" in Encyclopedia Of Telecommunications. John Willey, 2002.

[9]. S. William, cryptography and network security(2nd ed): principles and practice: Prentice- Hall,Inc., 1999

[10]. Pradeep Kumar Jaisal, Pankaj Kumar Mishra, "Survey of Security Issues in Wireless Adhoc Network Protocols",

IJECT VOL 2 Issue 4, Oct- Dec 2011, [Online] Available: http://www.iject.org/vol2issue4/pra deep1.pdf

[11]. S.Misra,I.Woungang and S.C. Misra, "Guide to Wireless Ad Hoc Networks", Springer science, 2009.

[12]. Ashwani Kush, Sunil Taneja and Divya Sharma, "Energy Efficient Routing for MANET", IEEE, 978-1-4244-9703-4/101, 2010.

[13]. L.M. Freeny, "Energy efficient communication in ad hoc networks", Mobile Ad Hoc Networking, Wiley-IEEE press, pp. 301-328, 2004.

[14]. N. Kumar Dr.C.Suresh Gnana Dhass "Power Aware Routing Protocols in Mobile Adhoc Networks-Survey", IJARCSSE Vol 2 Issue 9, Sep-2012, pp 121-128. Available online at: www.ijarcsse.com

[15]. Dr. Yogesh Chaba and Naresh Kumar Medishetti, " Routing Protocols in Mobile Ad hoc Network – A Simulation Study Final", JCS Vol 1. No. 1. August 2005.

[16]. Byung Jae Kwak, Nah-Oak Song, and Leonard E. Miller, "A standard measure of mobility for evaluating mobile adhoc network performance", IECE TRANS. COMMUN. E86-B, 2003.

[17]. T. Camp, J. Boleng, and V. Dvies, " A survey of mobility for ad hoc networks research, Wireless Communication and Mobile Computing(WCMC); Special issue on Mobile Ad hoc Networking: Research, Trends and Applications, pages pp. 483-502, 2002.

BIBLIOGRAPHY

K. Prabu has received his MCA, M.Phil from Annamalai University, Chidambaram, Tamilnadu, India in the year of 2006 and 2008. He is currently pursuing his Ph.D in Manonmaniam Sundaranar University, Tirunelvelli, Tamilnadu, India. At Present working as an Asst Professor in Dept of Computer Applications, Shree Ragavendra Arts & Science College, Chidambaram, Tamilnadu, India. His Research interested includes Ad hoc Networks. He is a life member of ISTE.

Dr. A. Subramani received his Ph.D Degree in Computer Applications from Anna University, Chennai. He is now working as a Prof & Head, Department of Computer Applications, K.S.R. College of Engg, Thiruchengode, Tamilnadu, India. His research interested includes ATM Networks, Ad Hoc Networks, High Speed Networks. He has published more that 32 technical papers at various National / International Conference and Journals. He is a life member of ISTE, CSI.