Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.240 – 245

RESEARCH ARTICLE

Routing Protocols in Ad-hoc Network

Ankita, Vikram Nandal

M.Tech Student, Department of CSE, R.N. College of Engineering & Management

Assistant Professor, Department of CSE, R.N. College of Engineering & Management

Sindhwaniankita@gmail.com, vikramcse@live.com

Abstract: ***The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organised networks. Ad hoc networks are simple peer-to peer networks, self-organized and with no fixed infrastructure. Ad-hoc network is a concept in computer communication which means that user wanting to communicate with each other forms a temporary network, without use of centralized administration. Each node in the network acts both as host and router and must therefore willing to forward packet for other node. For this purpose routing protocol is needed. A Mobile Ad-hoc Network (MANET) is a temporary wireless network composed of mobile nodes without any permanent infrastructure. Each node not only operates as an end system, it also acts as a router to forward packets on behalf of other nodes [1]. One of the best features of MANET is its flexibility and can configure itself in the fly and thus very suitable for the emergency situation***

Keywords: MANET, SEAD, ARIANE, MAC, flooding

1. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts which are also called nodes. In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centres i.e. it is decentralized. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Ad hoc is more to do with transmission of wireless signals from node to node dynamically rather than systematically. From this it comes out to be that Ad hoc network protocols act according to network situations. We can also suggest that an Ad hoc network is a computer-to computer temporary internet connection. It is often used to share files between two computers wirelessly. It is

actually a communication mode. The IEEE 802.11 MAC protocol [2] is a best choice for providing Ad-hoc network facilities. Mobile ad hoc network can be a standalone network or it is also possible to connect it to the infrastructure network. Thus it provides the facility to connect to the internet from anywhere. The proactive approaches attempts to maintain routing information for each node in the network at all times, where as the reactive approaches only find new routes when required and other approaches make use of geographical location information for routing.

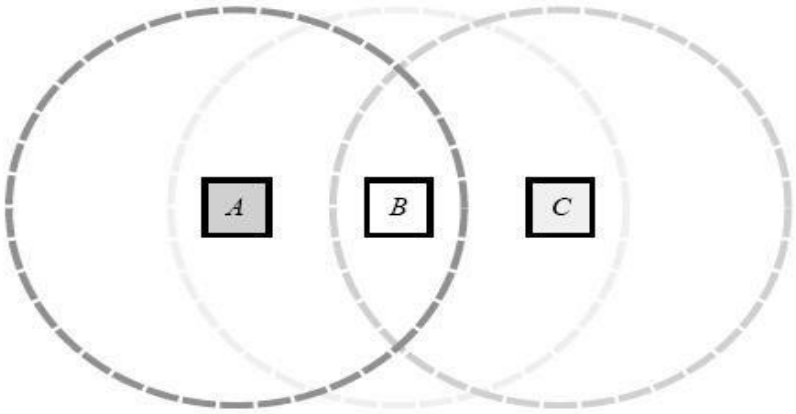

fig 1:simple MANET

2. Ad hoc Network

Ad hoc networks are a new paradigm of wireless communication for mobile hosts which are also called nodes. In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centres i.e. it is decentralized. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

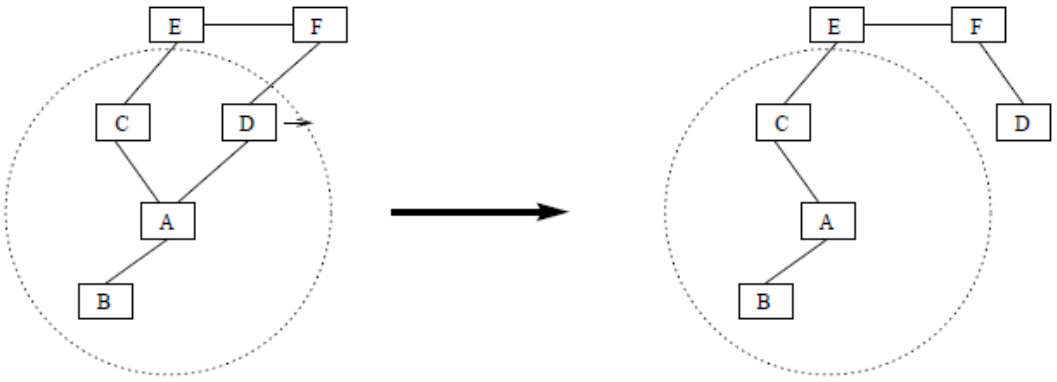

Fig 2:Ad hoc network

Features

- Nodes
    - Limited Resources: Battery Backup, Limited Range etc.
    - Dynamic Topology: Number of nodes keeps on changing on the fly.
    - Address Assignment: Allocating Address to different nodes successfully
- Wireless Channels
    - Relatively High Error Rate: High bit error rate is caused due to multipath fading, Doppler shift and signal attenuation.
    - High variability in the quality: Qos keep on changing as per the variability of network topology.
    - Low bandwidth.
    - Broadcast Nature: Every node has the ability to transmit info for path and information to all other adjacent nodes (e.g. FLOODYING).
    - Security Aspects: Authentication, Integrity, Availability.
- Ad hoc networks are basically peer-to-peer, multihop mobile wireless networks in which information packets are transmitted in a store-and –forward manner from a source to an arbitrary destination, via intermediate nodes.

3. Characteristics of MANET

MANETs are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a MANET

Dynamic Topologies

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

Energy Constrained Operation

Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy. The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

Bandwidth Constraint

Wireless links have significantly lower capacity [38] than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization.

Limited Physical Security

MANETs are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading [23], and denial of service type attacks.

4. Security Services in MANET

The ultimate goals of the security solutions for *MANETs* is to provide security services, such as *authentication, confidentiality, integrity, authentication, nonrepudiation, anonymity* and *availability* to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in *MANETs*. The common security services are described below.

Availability

Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or services of a distributed system. Availability ensures the survivability of network services despite of various attacks. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service [18].

Confidentiality

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Release of such information to enemies could have devastating consequences e.g. *ENIGMA*. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield. With respect to the release of message contents, several levels of protection can be identified.

Integrity

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message.

Authentication

Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [18].

Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. Nonrepudiation is useful for detection and isolation of compromised nodes. When node *A* receives an erroneous message from node *B*, nonrepudiation allows *A* to accuse *B* using this message and to convince other nodes that *B* is compromised.

Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network [18]. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system. It is very easy to make an island-hopping attack through one rough point in a distributed network.

5. Ad hoc Secure Routing Protocols

i) SEAD

SEAD is designed based on the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was proposed by Yih-Chun Hu, David B. Johnson and Adrian Perrig, [3].

DSDV: Destination Sequenced Distance Vector[10] routing protocol is one of the first protocol proposed for ad hoc wireless networks. It was developed based on the distributed Bellman Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It's a table driven routing protocol.

DSDV features

- It was developed on distributed bellmanford algorithm.
- First protocol used for Adhoc wireless network.
- Route to all destination are readily available at every node at all times.
- It provide loop free single path to destination

ii) Ariadne

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig [3], based on the Dynamic Source Routing protocol (DSR). [4][5][7].

DSR: DSR is an on-demand routing protocol, which finds the route as and when required, dynamically. DSR routing protocol manage the network without any centralized administrator or infrastructure. In route discovery this protocol discovers for the routes from source node to destination. In DSR, data packets stored the routing information of all intermediate nodes in its header to reach at a particular destination.
Ariadne uses the basic routing mechanism of DSR and uses TESLA [6] broadcasting authentication protocol. Ariadne provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the pair of communicating nodes. In Ariadne a route request packet (RREQ) contains eight fields: RREQ, initiator, target, id, time interval, hash chain, node list, and MAC list.

iii) Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP), was proposed by Papadimitratos and Hass [8]. SRP is implemented over DSR [4], [5], with an underlying Security Association (SA) between the source and destination nodes. The trust relation is maintained with a public key infrastructure and a shared key K(sd), was maintained between the source and destination nodes using the security association. In SRP the route request (RREQ) contains six fields and a MAC value to initiate the discovery process. The RREQ is signed with the shared key K(sd) between the source and destination.

References

[1] Xiang Chen, Hongqiang Zhai, Jianfeng Wang, and Yuguang Fang," TCP performance over mobile ad hoc networks", CAN. J. ELECT. COMPUT. ENG., VOL. 29, NO. 1/2, JANUARY/APRIL 2004.
[2] Stylianos Papanastasiou, Mohamed Ould-Khaoua, Lewis M. Mackenzie," On the evaluation of TCP in MANETs", Department of Computing Science University of Glasgow Glasgow, UK G128QQ.
[3] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "*Secure Efficient Ad hoc Distance vector routing*" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02) Panagiotis
[4] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edit). [2004]. *Mobile Ad Hoc Networking*: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354)
[5] C. Siva Ram Murthy and B.S. Manoj. [2004]. *Ad Hoc Wireless Networks, Architectureand Protocols*: 2004 Pearson Education (pp. 321-386, 473-526)
[6] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In *Network and Distributed System Security Symposium, NDSS '01*, pages 35–46, February 2001.
[7] David B. Johnson, David A. Maltz, and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop WirelessAd Hoc Networks", in Ad Hoc Networking, Editor: Charles E.Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
[8] Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[9] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "*A Secure Routing Protocol for Ad Hoc Networks*". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).

