ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

An Overview of Wireless Ad-hoc Networks

Jyotirmoy Das
Assistant Professor, Department of Information Technology
Gauhati Commerce College, Guwahati, India

Prakash Das
Department of Computer Science, M.C.A.
NERIM , Guwahati, India

Abstract: Ad hoc network is a collection of nodes that is connected through a wireless medium forming dynamically changing topologies. A considerable effort has been put into studying ad hoc networks over the past decade. Many routing protocols at different layers have been proposed and studied. In this paper, we discuss about some of the most popular protocols that follow the table-driven and the source-initiated on-demand approaches and a few others, their challenges and also discuss the future scope of ad hoc networks.

Keywords: Ad hoc Network, Wireless, Routing Protocols, Table-driven, On-demand

I. INTRODUCTION

Wireless Ad hoc Networks (WANET) does not rely on any pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. They are decentralized in nature where each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Ad hoc networks are self-configurable systems and support movability and organize themselves arbitrarily. This refers to the fact that the topology of the ad hoc network changes dynamically and unpredictably.

In other words, an ad hoc network typically refers to any set of networks where all devices have equal status on a network. Moreover, they are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks [1].

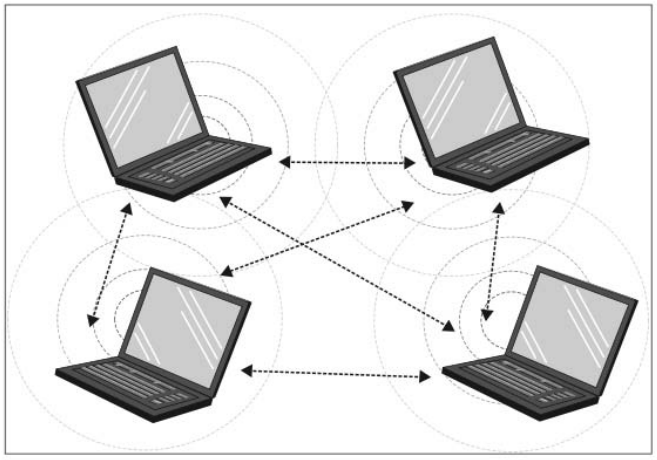

Fig 1: Example of an ad hoc network [2]

II. HISTORY

The Defense Advanced Research Project Agency (DARPA) initiated research of using packet switched radio communication to provide reliable communication between computers. The introduction of Packet Radio Network(PRNET) and Survivable Adaptive Radio Networks (SURAN) from early 1970s to mid 1980s provided packet switched networking to battlefields or hostile environments by forming nodes in the network. Approaches such as ALOHA and CSMA were considered for the PRNET to perform and later SURAN significantly improved the radio performance and also provided resilience to electronic attacks. In the early 1990s a new phase in ad hoc networking was seen when Notebook computers along with Open Source programs became popular in the commercial market. It was during this time that the idea of an infrastructure-less collection of mobile hosts was proposed and the IEEE 802.11 subcommittee adopted the term “ad hoc networks.” The first generation of ad hoc networks is called Packet Radio Network (PRNET). Around the same time, United State Department of Defence (DOD) continued funding for programs such as Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR) [3],[4]. With GloMo, it was possible to set up an Ethernet-type multimedia connectivity for handheld devices anytime, anywhere. Several routing schemes were developed during this time and several topologies were experimented. CSMA/CA and TDMA were some of the popular approaches used for GloMo. The NTDR was self-organized into a two-tier ad hoc network which used clustering and link-state routing. Today NDTR is the only non protypical ad hoc network in use and is used by the U.S. Army. A good number of commercial standards and activities have evolved since the mid 90s which has led to the growth of ad hoc network development.

III. ROUTING PROTOCOLS FOR AD HOC NETWORKS

There are numerous protocols defined for ad hoc networks which differ in their algorithmic implementation. Each of these protocols are designed to perform as well as possible according to the situation and environment The chosen protocol for any netwok must cover all states of a specified network and must consume only a minimum amount of network resources. In the following section we categorize these protocols and discuss a few of them according to their category :

A Table-driven (proactive) routing :

Proactive routing maintains routing tables at each node and these routing tables are updated periodically [5, 11]. They work similar to the traditional wired network routing protocols. These protocols are not feasible for large number of networks because bandwidth consumption can turn up to be an issue as the routing tables gets more and more complicated with routing information. The examples of different varieties of table driven protocols are given below:

- Destination Sequenced Distance vector routing (DSDV) – The DSDV protocol requires each node to advertise its own routing table to each of its current neighbors. The advertisement must be made frequently as the entries in this list may change dynamically over time. Moreover, each node agrees to relay data packets to other nodes upon request. The protocol also has the ability to determine the shortest number of hops for a route to a destination and this is important because inactive systems should be avoided. In this way a mobile computer may exchange data with any other mobile computer in the group even if the target of the data is not within range for direct communication.

- Optimised Link State Routing Protocols (OLSR) –

  OLSR is an optimization of the link state protocol for ad hoc networks. It is proactive in nature and hence it has an advantage of having routes immediately available when needed.. Here, instead of all links, only a subset of links are declared. The flooding is also controlled by using only selected nodes in the network. This protocol is designed to work in a completely distributed manner and thus does not depend upon any central entity. It performs hop by hop routing.i.e. each node uses its most recent information to route a packet.

- Wireless Routing Protocol (WRP) –

  The protocol introduces mechanisms which reduce route loops and ensure reliable message exchange. WRP is an enhanced version of the Destination Sequenced Distance vector routing (DSDV), and it inherits the properties of the distributed Bellman–Ford algorithm to calculate paths in the network. To counter the count-to-infinity problem and to enable faster convergence, The protocol maintains information regarding the shortest distance to every destination node in the network and the next-to-last hop node on the path to every destination node. Similar to DSDV, this protocol also maintains an up-to-date view of the network, and so every node has a readily available route to every destination node in the network. WRP uses a set of tables rather than only one topology table, to maintain more accurate information than DSDV. The tables maintained by a node in WRP are distance table (DT), routing table (RT), link cost table (LCT), and a message retransmission list (MRL) [6].

B. On-demand (reactive) routing

Reactive protocols do not maintain the routing information of the network topology as Proactive protocols do. These set of protocols collect all the necessary information of the topology only when it is required by a node for communication. This type of protocols finds a route on demand by flooding the network with Route Request packets. Examples of on-demand algorithms are:

- Ad Hoc On Demand Distance Vector Routing Protocol (AODV) – The AODV protocol dynamically establishes route table entries at intermediate nodes. It uses a broadcast route discovery mechanism (also used in DSR) algorithm. This protocol is good with networks with many nodes where a large overhead is incurred by carrying source routes in each data packet. The participating nodes stores only the routes that are necessary. Also the need for broadcast is minimized as well as it reduces memory requirements and redundancy [1,5].

- Temporally Ordered Routing Algorithm (TORA) –

  This includes the non-hierarchical routing algorithm from which a high degree of scalability is achieved. Here, the generation of far-reaching control message propagation is to be suppressed. For achieving this, a Directed Acyclic Graph (DAG) is build and maintained by TORA. Flowing of information is from nodes with higher heights to nodes with lower heights. TORA achieves loop-free multipath routing by maintaining a set of totally ordered heights at all times. It should be noted that information cannot 'flow uphill' and so cross back on itself. Localization of control messages to a very small set of nodes near the occurrence of a topological change is the key design concepts of TORA. To accomplish this, the protocol performs three basic functions these are the Route creation, Route maintenance and Route erasure.

- Dynamic Source Routing Protocol (DSR) –

  It is the simple and efficient routing protocol which is designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Thus, network is completely self-organizing and self-configuring. Here, no existing network infrastructure or administration is required. Network nodes cooperate to forward packets for each other. This is done in order to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another. All routing is automatically determined and maintained by the DSR routing protocol, as nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change. The resulting network topology may be quite rich and rapidly changing, since the

number or sequence of intermediate hops needed to reach any destination may change at any time.

C. Hybrid (both proactive and reactive) routing :

It combines the best features of the first two categories. The Zone Routing Protocol (ZRP) is one of the hybrid routing protocols : Here, every network node proactively maintaining routing information about its routing zone, while reactively acquiring routes to destinations beyond the routing zone.
The Independent Zone Routing Protocol (IZRP), an enhancement of the Zone Routing Protocol, allows adaptive and distributed configuration for the optimal size of each node's routing zone, on per-node basis
The advantages of proactive and reactive routing are combined in Hybrid Protocols. In the initial phase , pro-active routing is used to establish the routing and later the requirements are fulfilled by employing reactive flooding.
Examples of hybrid algorithms are:

- ZRP (Zone Routing Protocol) –

  ZRP uses IARP as pro-active and IERP as reactive component. It is important to note that Proactive routing uses excess bandwidth to maintain routing information, while Reactive routing involves long route request delays. Reactive routing also inefficiently floods the entire network for route determination. The main objective of the Zone Routing Protocol (ZRP) is to address the problems by combining the best properties of both approaches. ZRP can be classed as a hybrid reactive/proactive routing protocol. It reduces the proactive scope to a zone centered on each node. The maintenance of routing information is easier in a limited zone. Also, the amount of routing information that is never used is minimized [7, 12]. Route requests can be more efficiently performed without querying all the network nodes, since all nodes proactively store local routing information.

D. Hierarchical routing protocols

Here, the nodes are grouped into some clusters in such a way that each cluster has its own cluster head. These cluster heads are used for higher level communication reducing the traffic overhead. Thus, this helps in reducing the size of the routing tables, thereby helping in providing better scalability. It should be noted that the choice of proactive and of reactive routing depends on the hierarchic level in which a node resides. Initially, the routing is established with some proactive routing protocol and later reactive flooding is performed on the lower levels [7]. Examples of hierarchical routing algorithms are:

- CBRP (Cluster Based Routing Protocol) :

  Here, the nodes of a wireless network are divided into several disjoint or overlapping clusters. This is done in such a way that each cluster elects one node as the so-called clusterhead. These special nodes are responsible for the routing process. However, the clusterheads are able to communicate with each other by using gateway nodes. Note that a gateway is a node that has two or more clusterheads as its neighbours or— when the clusters are disjoint—at least one clusterhead and another gateway node [8, 10].

The routing process itself is performed as source routing by flooding the network with a route request message. There will be less traffic due to the clustered structure. This is because route requests will only be passed between cluster-heads. In order to support the cluster formation process each node uses a neighbor table, which is used for the storage purpose of information about its neighbour nodes. These informations could be their ID's, their role in the cluster (clusterhead or member node) and the status of the link to that node (uni-/bi-directional).

IV. SECURITY CHALLENGES IN ADHOC NETWORK

It is very much important to note that Ad-hoc networks are highly vulnerable to security attacks. Today, dealing with this is one of the main challenges of developers of these networks. Following are the main reasons for this difficulty:

1) Shared broadcast radio channel,
2) Insecure operating environment,
3) Lack of central authority,
4) lack of association among nodes,
5) Limited availability of resources, and
6) Physical vulnerability

SECURITY GOALS FOR AD HOC

Availability, confidentiality, authentication, integrity and non-repudiation are the four headings under which the security of a network is examined.

a) **Availability** refers to the fact that the network must remain operational at all times despite denial of service attacks.
b) **Confidentiality** ensures that certain information is never disclosed to certain users.
c) **Authentication** is the ability of a node to identify the node with which it is communicating.
d) **Integrity** guarantees that a message is never corrupted when transferred.
e) Non-repudiation states that the sender of the message cannot deny having sent it.

SECURITY BREACHING/BREAKING :

Ad hoc network susceptible to certain link attacks. These attacks can range from passive eavesdropping to active impersonation, message replay and message distortion.
Eavesdropping refers to allowing the attacker access to secret information, hence, violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages, thus violating authentication, nonrepudiation, availability and integrity.

Thus, security can be breached by the following ways :

i) **Vulnerability of Channel : M**essages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

ii) **Vulnerability of nodes:** The network nodes can more easily be captured and fall under the control of an attacker, since they usually do not reside in physically protected places, such as locked rooms.

iii) **Absence of Infrastructure:** An ad-hoc network has extra security requirements caused by its lack of proper infrastructure. These networks are supposed to operate independently of any fixed infrastructure. Here, accountability is very difficult to determine as there is no central authority which can be referenced when it comes to making trust decisions about other parties in the network [9].

iv) **Dynamic relationship between the nodes**: This leaves very little opportunity for the nodes to form trust relationships with each other. Nodes must act as both terminals and routers for other nodes in an ad-hoc network. As there are no dedicated nodes, there is a need of a secure routing protocol. Here, multi hop routing protocols are usually employed. These can lead to several problems due to non-cooperating nodes and denial of service attacks.

SECURITY ATTACKS

Denial of Service: These attacks aim at the complete disruption of the routing function and thus, the entire operation of the ad hoc network [9].

Following are the two specific instances of denial of service attacks –

a) Routing table overflow –
In this attack, the malicious node floods the network with undesirable or harmful route creation packets. This is done in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes.

b) Sleep deprivation torture -
This attack aims at the consumption of batteries of a specific node. This is done by constantly keeping it engaged in routing decisions.

Routing Table Poisoning:
Creation of false entries in the tables of the participating nodes became possible as the routing protocols maintain tables that hold information regarding routes of the network. This occurs in poisoning attacks where the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes.
Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops and bottlenecks [9].

Rushing Attack: This attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols.
There exists a Rushing Attack Prevention (RAP) which is a generic defence against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol. This allows that protocol to resist the rushing attack [9].

Breaking the neighbour relationship: In this process, an intelligent filter is placed by an intruder on a communication link between two information systems. These could modify or change information in the routing updates [9].

Masquerading: This refers to gaining unauthorized access to personal computer information through legitimate access identification. Thus, the masquerade attacker compromises the authentication system attaching itself to the communication link and illegally joining in the routing protocol [9].

Passive Listening and traffic analysis:
It is very important to note that the exposed routing information could be gathered passively by the intruder. This type of attack cannot effect the operation of routing protocol. However, it is a breach of user trust to routing the protocol. Hence, sensitive routing information should be protected[9].

V. THE FUTURE

At present, research in ad hoc network is enjoying unprecedented interest. They are no longer viewed as stand-alone group of wireless terminals. Ad hoc networks are expected to provide opportunities for utilization of network applications, yet many issues still have to be addressed. Dealing with security attacks is one of the main challenges of the researchers and developers of ad hoc networks. As discussed previously, ad hoc networks suffer from the lack of central authority , also it has an insecure operating environment which brings in front many questions about the security and privacy of information across such a network. Also, most research related to ad hoc network models where all the nodes participating in the network are within a mutual range, are considered to be fairly simple; otherwise, the nodes are required to relay data from some data source to accomplish data delivery. Different routing protocols are used for such information exchange which perform similarly (but on a small scale) as the Internet routers do within the backbone of the Internet. In both cases, packets have to be relayed (forwarded) towards the destination, after information has been acquired and exchanged so that a useful route can be determined. Continuous efforts have been made and experiments and analysis are performed in order to develop better and new versions of protocols for the purpose. It is often said that ad hoc networks are the future of wireless networks because of their versatility, simplicity, and ease of use and above all it is less expensive as compared to any other forms of networking. It is predicted that the nodes in an ad hoc environment will get smaller, cheaper and more capable as research and development in technology is taking its pace quite rapidly. Technologies such as Wireless LAN, Bluetooth etc. will probably be more popular for connecting appliances to the Internet. Mesh-based solutions will gain popularity and may even be the dominant solution. Multimedia application support

for Military ad hoc networks will be another aspect to look at. Moreover ad hoc networks in Military will have higher capacities, be more adaptive, and construct multimedia-networked system for battlefield elements.

VI. CONCLUSION

The area of ad hoc networks is a very fast growing area and it has its own advantages as well as disadvantages. We have seen how easy and simple ad hoc networks are when it comes to setting up or configuring the network but it is also true that as the network expands, routing and managing becomes difficult. Researchers and developers have been devoting much of their time in achieving routing stability and positive results have been witnessed in recent times as many problems related to routing has disappeared. Also researchers have been looking beyond existing design paradigms to make successful models of wireless communication through ad hoc properties.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_ad_hoc_network

[2] http://2.bp.blogspot.com/-HSqzW4lwFiI/T0MUOhW9NjI/AAAAAAAAAEU/1dFW8mMsEng/s1600/Wireless_ad_hoc.png

[3] Anders Lindgren, Kaustubh S. Phanse, Tomas Johansson, Robert Brannstrom, Christer Ahlund, "Future Directions in Ad hoc Networking Research" 5th Scandinavian Workshop on Wireless Ad-hoc Networks: ADHOC ´05. Stockholm : Wireless at KTH, Royal institute of technology, 2005.

[4] Ram Ramanathan, Jason Redi,"A Brief Overview of ad-hoc networks : Challenges and Directions", IEEE Communications Magazine Vol. 40, Issue 5, May 2002

[5] Dr. Renu Dhir ,Vanita Rani, "A Study of Ad-Hoc Network: A Review " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 3, March 2013

[6] Petteri Kuosmanen, "Classification of Ad Hoc Routing Protocols" Petteri Kuosmanen "Classification of Ad Hoc Routing Protocols", Finnish Defence Forces Naval Academy P.O. Box 5, FIN-00191 Helsinki, Finland.

[7] Nicklas Beijar, "Zone Routing Protocol (ZRP)" , Networking Laboratory, Helsinki University of Technology , P.O. Box 3000, FIN-02015 HUT, Finland, Nicklas.Beijar@hut.fi

[8] Tim Daniel Hollerung, "The Cluster-Based Routing Protocol", project group Mobile Ad-Hoc Networks Based on Wireless LAN, University of Paderborn, 2003/2004.

[9] Karan Singh,Rama Shankar Yadav, Ranvijay , "A Review Paper on Ad hoc Network Security", International Journal of Computer Science and Security, Volume (1): Issue (1)

[10] Tim Daniel Hollerung, "The Cluster-Based Routing Protocol", project group Mobile Ad-Hoc Networks Based on Wireless LAN, University of Paderborn, 2003/2004.

[11] Dr. Renu Dhir ,Vanita Rani, "A Study of Ad-Hoc Network: A Review " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 3, March 2013

[12] Nicklas Beijar, "Zone Routing Protocol (ZRP)" , Networking Laboratory, Helsinki University of Technology , P.O. Box 3000, FIN-02015 HUT, Finland, Nicklas.Beijar@hut.fi