Reviewing on Ad Hoc wireless Network

Ashish Chaturvedi, Sashi Kant Gupta, Aamer Mohammad

Research Scholar, ITM University, Gwalior. Asst. Prof, ITM University, Gwalior. Asst. Prof, ITM University, Gwalior

E-mail: achaturvedi51@gmail.com, skgitm@gmail.com, aamir.mahammad.1711@gmail.com

Abstract

This paper presents a coherent survey on ad hoc wireless networks, with the intent of serving as a fast reference to the current research issues in ad hoc network. The paper discusses a broad range of research issues such as Routing, Medium Access, Multicasting, Quality of service, TCP performance, Energy, Security, outlining the major challenges which have to be solved before widespread deployment of the technology is possible. Through this survey it would be seen that Ad hoc Networking presents an interesting research area inheriting the problems of wireless and mobile communications in their most difficult form.

Key words: Ad hoc network, routing, MAC, multicasting, quality of service, TCP, energy, security

1. Introduction

AD HOC networking promises to provide the technical concepts for a variety of future wireless systems and services, such as short-range data transfer, vehicular communication, robust emergency services, and multihop access to infrastructure [4]. An ad hoc network connects mobile devices, referred to as nodes, which act as relays to provide a communication between remote nodes in a multi-hop fashion. A wireless ad hoc network is a network where nodes can communicate with each other without the support of fixed infrastructure or central administration [7]. Communication is directly between nodes or through intermediate nodes acting as routers. It can be set up easily and quickly with low cost. The deployment of wireless networks where there is no infrastructure or the local infrastructure is not reliable can be difficult. Ad hoc networks have been proposed in order to solve such problems. The main advantages of ad hoc networks are rapid deployment, flexibility, low cost, and robustness. Ad hoc networks can be easily set up, even in desert places and can endure to natural catastrophes and war. These characteristics make ad hoc networks well suited for military activities, emergency operations, disaster recovery, large scale community networks, and small networks for interaction between meeting attendees or students in a lecture room. The vision of wireless ad hoc networks is wireless Internet, where users can move anywhere at any time and still remaining connected with the rest of the world. The successful implementation of ad hoc wireless networking technology presents a unique set of challenges that differ from traditional wireless systems and wired networks.
This paper discusses the research issues which are being generated by these challenges and as such present a detailed overview of ad hoc networking.

2. Ad hoc MAC protocols issues

There are basically two main categories of MAC protocols: first is Random Access Protocols—where nodes compete with one and other to get full access to the shared medium and second is Controlled Access Protocols—where an infrastructure or Master node decides which node get access to the medium [2]. The lack of infrastructure and the peer-to-peer nature of ad hoc networking make Random Access Protocols the natural choice for medium access control in ad hoc network. Thus most ad hoc MAC protocols are based on the random access paradigm. Example includes MACA (Multiple Access with Collision Avoidance), MACAW (MACA with Acknowledgment), MACA-BI (MACA by Invitation), DBTMA (Dual Busy Tone Multiple Access) and FAMA (Floor Acquisition Multiple Access) [5]. Among these protocol CSMA/CA (carrier sense multiple access with collision avoidance) a variant of MACA was selected by IEEE 802.11 Committee as the basis for its standard due to its inherent flexibility and because it solves expose and hidden terminal problem by RTS-CTS-DATA-ACK handshake. MAC Controlled Access Protocol examples TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access), CDMA (Code Division Multiple Access) and TSMA (Time Spread Multiple Access) though seldom used in ad hoc networks are preferred in environments that needs Quality of Service (QoS) guarantee as their transmissions are collision free. Their applications are mainly adapted to Bluetooth and cluster-based ad hoc networks where access to the shared medium is control by Master nodes. Optimization to improve the performance of ad hoc MAC protocols include algorithms to minimize mobile node energy consumption, like allowing nodes to sleep during the period, they are idle and in the incorporation of directional antenna. Typically ad hoc network nodes assume the use of Omni-directional antennas. With Omni-directional antenna, while two nodes are communicating over a given channel, the MAC protocol requires that all other nodes in the vicinity stay silent. But with directional antenna, two pairs of nodes in the network located in each other’s nearby may potentially simultaneously access the channel, depending on the directions of transmission. Directional antennas can adaptively select interested radio signals in specific directions, while rejecting out unwanted interference from other directions. This can increase power gain of the wireless channel, in addition to higher spatial reuse.

3. Deafness Problem

By using Omni-directional antennas for the nodes in the network. So during transmission, all nodes in the neighborhood of a sender or a receiver are expected to keep silent to avoid collision or interference with the ongoing transmission. This leads to low spatial reuse. On the other hand, when directional
antennas are used, we can allow several transmissions at the same time without interfering with each other. Thus, the spatial reuse can be highly improved. The transmission range can also be increased because of the larger antenna gain and less interference.

However, when we use directional antennas, deafness is a severe problem. This happens when a node sends an RTS to the intended receiver but gets no response [8]. Then the sender wills double its contention window and then back off. If the intended receiver is busy in a long data transmission, the sender will fail to get CTS for several times. After the receiver completes its transmission and becomes idle, the sender will have a large contention window and may probably have chosen a very long back off period. So the channel will be idle for a long time. The worse case occurs when the sender drops the packet because it has exceeded the maximum number of unsuccessful attempt.

“Deafness occurs when the transmitter fails to start communication with its intended receiver, because the receiver’s antenna is oriented in a different direction.”

Table 2.1: Comparison of Omni-directional antennas MAC Protocols in Ad-Hoc Networks

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Carrier Sensing</th>
<th>RTS/CTS</th>
<th>Increased RTS/CTS Transmission Time</th>
<th>Back-off Algorithm</th>
<th>Split channel</th>
<th>Busy Tone based</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMA/CA</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>BEB</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FAMA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>BEB</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MACA / MACAW</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>BEB/MILD</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IEEE 802.11 MAC</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>BEB</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
2.2: Comparison of directional antennas MAC Protocols in Ad-Hoc Networks

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Basic Protocol</th>
<th>Carrier Sensing</th>
<th>Omni directional RTS/CTS</th>
<th>Directional RTS</th>
<th>On-Demand Location Tracking</th>
<th>Directional Busy Tone</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBTMA/DA</td>
<td>DBTMA</td>
<td>No</td>
<td>RTS/CTS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MAC / DA1</td>
<td>802.11</td>
<td>Yes</td>
<td>CTS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MAC / DA2</td>
<td>802.11</td>
<td>Yes</td>
<td>RTS/CTS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

4. Ad hoc routing protocols

The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to the destination [9]. Ad hoc routing protocols are typically subdivided into two main categories: Proactive (Table-Driven) Routing Protocols and Reactive (On-Demand) routing protocols [10]. Proactive routing protocols are derived from legacy Internet distance-vector and link-state protocols. They maintain tables that store routing information. In order to maintain a consistent network view and for any change in network topology, they triggers propagating updates throughout the network. The advantage is that routes to any destination are always available without the overhead of a route discovery but such Protocols cannot perform properly when the mobility rate in the network is high or when there are a large number of nodes in the network. Protocols in this category differ in the number of tables they contain as well as on the details of how they are updated. For example, nodes in Destination-Sequenced Distance Vector (DSDV) algorithm maintain route information to each and every other node in the network. As the network status changes full updates are exchange among all nodes. The Wireless Routing Protocol (WRP) localizes the updates to the immediate neighbors. The Cluster Gateway Switch Routing (CGSR) protocol reduces the size of the tables and amount
of information propagation by having each cluster of nodes elect a cluster head. Network-wide information is only exchanged among the cluster heads. While the amount of information propagation is reduced, this results in inefficient routes. The Fisheye State Routing Protocol has been recently suggested, this differ from others in that the update frequency is inversely related to the distance between any two nodes.

On-Demand routing protocols are characterized by a path discovery mechanism that is initiated when a source needs to communicate with a destination that it does not know how to reach. The Route Discovery is usually in the form of query flood. Generally, on-demand routing requires less over-head than table-driven routing; but it incurs a path discovery delay whenever a new path is needed.

The differences between on-demand protocols are in the implementation of the path discovery mechanism and optimizations of it. Dynamic Source Routing (DSR) uses source routing, with every packet carrying the full path information with it. Similarly, Ad hoc On-Demand Distance Vector Routing Protocol (AODV) is an on-demand version of DSDV where the path results in exchange of the portions of the routing table necessary for establishing the route. Other on-demand algorithms include Temporally Ordered Routing Algorithm (TORA) that discovers multiple paths from a source to destination and re-initiates discovery only when all of them have failed.

Associability-Based Routing (ABR) incorporates route quality by preferring hops that have been static for a long period. Similarly, Signal Stability Routing (SSR) prefers routes with strong received signal power. In addition to proactive and reactive protocols are hybrid protocols. The Zone-Based Hierarchical Link State Routing Protocol (ZRP) is an example of hybrid protocol that combines both proactive and reactive approaches thus trying to bring together the advantages of the two approaches. ZRP defines around each node a zone that contains the neighbors within a given number of hops from the node. Proactive algorithm is used by a node to maintain route to all other nodes within its zone and reactive algorithms are used by the node to determine routes to nodes outside it zone. Presently, TORA, DSR, AODV and ZRP are the four protocols currently under study by the IETF MANET working group as candidate protocols for evaluation and standardization.

5. Ad hoc multicasting

Multicasting is the transmission of data grams to a group of zero or more hosts identified by a single destination address. Ad Hoc wireless network find application in civilian operations (collaborative and distributed computing), emergency search-and-rescue, law enforcement, and warfare situations, where setting up and maintaining a communication infrastructure may be difficult or costly. Multicast routing protocols play an important role in ad Hoc wireless network to provide this communication [11, 12].
Multicast protocols for ad hoc wireless networks are broadly classified into two types: application independent/generic multicast protocols and application dependent multicast protocol. While application independent multicast protocols are used for conventional multicasting, application dependent multicast protocols are meant only for specific applications for which they are designed.

6. Quality of service (QoS)

Due to the broadcast and dynamic nature of Ad hoc Networks, providing Quality of Service (QoS) other than best effort, is a very challenging task [13]. But QoS is important for the ad hoc network to interconnect with wired networks which support QoS (e.g. ATM, Internet, etc.) and for real time applications. To support QoS, the link state information such as delay, bandwidth, loss rate, cost and error rate in the network should be available and manageable. However, getting and managing this link state information is very difficult. Because of resource limitations, mobility and random joining and leaving of network nodes.

Quality of service is the performance level of service offered by the network to the users. The goal of the QoS provisioning is to achieve a more deterministic network behavior, so that information created by the network can be better delivered and network resources can be better utilized [14]. Several issues, such as the service model, routing strategies, admission control, resource reservation, signaling techniques, and MAC protocols need to be considered in the context of providing QoS in ad hoc wireless networks. In fact, every layer of the network has to be made QoS aware because only when all the factors are considered together in the overall scenario can effective QoS be provided for the end-user application.

A QoS service model specifies an overall architectural framework, within which certain types of services can be provided in the network. Some of the prominent service models suggested for ad hoc networks are: flexible quality of service model for MANETs (FQMM), cross layer service model, and stateless model for wireless ad hoc networks (SWAN).

Signaling is used in order to negotiate, reserve, maintain and free up resources, and is one of the most complicated aspects of the network. It should be performed reliably (including topology changes) with minimum overhead. Out-of-band and in-band signaling are two commonly used approaches.

If the application needs to be guaranteed a certain minimum bandwidth or end-to-end delay, the routing scheme should also be QoS aware. Not only does the route have to be valid at the time the data is to be transported, but also all the nodes along that route need to have sufficient resources in order to support the QoS requirement of the data flow and the application.

QoS routing refers to the discovery and maintenance of routes. These routes can fulfill QoS objectives under given resource constraints [15]. A QoS routing protocols should work together with QoS signaling for establishing paths through the network that meet end-to-end QoS requirements, such as bandwidth demand delay or delay jitter bounds, or multi-metric constraints.
Once a potential route is established, it is necessary to reserve and allocate the required resources in all the nodes of that route so that the demands of the application can be met. The **admission control** becomes important in this context.

**QoS resource reservation signaling:** QoS Signaling is the process of setting up a connection from the source to the destination that involves reservation of resources in the intermediate nodes. QoS Signaling acts as a control center in QoS support to the network. It reserve and release resources, tear down, setup and renegotiate flows in the networks. QoS Signaling systems can be divided into two types of signaling, first is in-band signaling and the other is out-of-band signaling. In in-band signaling, control information is piggybacked within data packets while in out-of-band signaling control information are sent as explicit packets.

**QoS medium access control (MAC):**
QoS MAC Protocol solves the problems of medium contention, hidden and expose terminal problem, supports reliable unicast communication and provides resource reservation for real-time traffic management in a distributed wireless environment. Among many MAC protocols and improvements that have been designed for QoS, these protocols can provide QoS guarantees to real time traffic management in a distributed wireless communication environment include GAMA/PR protocol and Black-Burst (BB) contention mechanism.

7. **Transport layer protocol**

The main objective of transport layer protocols [3] include setting up and maintaining end-to-end connection, reliable end-to-end delivery of data packet, flow control and congestion control. There exist simple connections less transport layer protocols (UDP) which neither perform flow control and congestion control nor provide reliable data transfer [17]. Such unreliable connectionless transport layer protocols do not take into the account of current network status such as congestion at the intermediate link, the rate of collision, or other similar factor affecting the network throughput.

The major performance degradation faced by a reliable connection-oriented transport layer protocol such as transmission control protocol (TCP) in ad hoc wireless network arises due to frequent path break, presence of state routing information, high channel error rate and frequent network partition. TCP is an effective connection-oriented transmission control protocol that provides the essential flow control and congestion control required to ensure reliable packet delivery [16]. TCP was originally designed to work in fixed networks. Because error rate in wired network is quite low, TCP uses packet loss as an indication for network congestion and deals with this effectively by making corresponding transmission adjustment to its congestion window.

TCP as the transport layer protocol, due to the mobility of nodes and limited transmission range, an existing path to a destination node experience frequent path break. Each path break result in route reconfiguration
that depends on the routing protocol employed. The processes of finding an alternate path or reconfiguring the broken path might take longer than the retransmission time out of the transport layer at the sender, resulting in retransmission of packets and execution of the congestion control algorithm.

Due to mobility of the nodes, ad hoc wireless networks frequently experience isolation of nodes from the rest of the networks or occurrence of partitions in the network. If a TCP connection spans across multiple partitions, that is, the sender and receiver of the connection are in two different partitions, all the packets get dropped. This tends to be more serious when the partitions exist for a long duration, resulting in the multiple retransmissions of the TCP packets and subsequent increase in the retransmission timer. Such a behavior cause long periods of inactivity even when a transmit partition in the network lasts for a short while.

8. Energy Management

Energy management is defined as the processes of managing the source and consumers of energy in a node or in the network as a whole for enhancing the life time of the network energy management can be classified in to following category [18].

Transmission power management: the power consumed by the radio frequency module of a mobile node is determined by several factors such as the state of operation, the transmission power, and the technology used for RF circuitry. The state of operation refers to transmit, receive and sleep modes of the operation. The transmission power is determined by the reachability requirement of the network, the routing protocols and MAC protocols employed.

Battery power management: the battery management aimed at extending the battery life of a node by taking advantage of its chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy [19]. Recent study showed that pulsed discharge of a battery gives longer life than continuous discharge. Controlling the charging rate and discharging rate of battery is important in avoiding early charging to the maximum charge or full discharge blow the minimum threshold.

Processor power management: the clock speed and the number of instructions executed per unit time are some of the processor parameter that affects power consumption. The CPU can be put into different power saving modes during low processing load conditions. The CPU power can be completely turned off if the machine is idle for a long time. In such cases interrupts can be used to turn on the CPU upon detection of user interaction or other events.

Device power management: intelligent device management can reduce power consumption of a mobile node significantly. This can be done by the operating system by selectively powering down interface device that are not used or by putting devices into different power saving modes, depending on their usage.
9. Security

Performing communication in free space and the broadcast nature of ad hoc networks open it for security attacks [6]. Ad hoc wireless links are susceptible to attacks that are ranging from passive eavesdropping to active impersonation, message distortion and message replay. Active attacks might allow the opponent to delete messages, inject erroneous, modify messages and impersonate a node, thereby violating availability, integrity, authentication and nonrepudiation [20]. Understanding possible form of attacks is always needed because it is the first step for developing good security solutions. Two types of security mechanisms can be generally applied are preventive and detective. Preventive mechanisms are mainly based on secret key cryptography (key-based cryptography). However, designing secure key distribution that allows the creation of unforgettable credentials in ad hoc networks is a challenging problem. Daffy–Hellman key exchange may indeed help to establish some temporary security between particular endpoints. However, they are also vulnerable to the man-in-the-middle attacks. The major security threats that exist in ad hoc wireless networks are as follows:

**Denial of service:** The attack affected by making network resource unavailable for service to other node, either by consuming the bandwidth or by overloading the system, is known as denial of service (DoS).

**Resource consumption:** The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resource available in the network.

**Host impersonation:** A compromised internal node can act as another node and respond with appropriate control packets to create wrong route entries, and can terminate the traffic meant for the intended destination node.

**Information disclosure:** A compromised node can act as an informer by deliberate discloser of secret information to unauthorized nodes. Information like the amount and the periodicity of traffic between a selected pair of nodes and pattern of traffic changes can be very valuable for military applications. The use of filler traffic (traffic generated for the sole purpose of changing the traffic pattern) may not be suitable in resource-constrained ad hoc wireless network.

**Interference:** A common attack in defense applications is to jam the wireless communication by creating a wide-spectrum noise. This can be done by using a single wide-band jammer, sweeping across the spectrum. The MAC and the physical layer technologies should be able to handle such external threats.

10. Conclusion:

In this paper, we have tried to survey ad hoc network mainly from a technical point of view. We have discussed some of the typical research issues of ad hoc networks, such as routing algorithms, MAC protocols, security, QoS etc. This paper provides the fastest study of ad hoc network with various research issues. These issues may be used for further research work for improving the network’s performance.
Reference:

5. Sunil Kumar, Vineet S. Raghavan, Jing Deng, “Medium Access Control protocols for ad hoc wireless networks: a survey”
7. C. Shiva Ram Murthy, B. S. Manoj, “ad hoc wireless network”