Erkaboy K. Samandarov,
Lecturer,
Tashkent State Pedagogical University

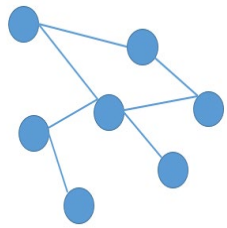
Wireless Mesh Network

Key words: *wireless mesh network (WMN), IEEE, MIMO, 3G, CSMA, ALOHA, QoS, MAC, TDMA, MANETs, DSR, AODV.*

Annotation: *IT (Information Technologies) have also developed like other fields because of great changes in the history of humanity in the last two decades. Devices which are in the new form (smartphones, laptops and tablets) are created. Above devices user can be used any condition. As a result, the requirement had appeared the flexible computer networks. Wireless Mesh Networks (WMNs) can be used dependents on locating the positions of user. In this paper we overview WMNs. Moreover, we consider the architecture of WMNs and routing protocols for WMNs. We consider the architecture of WMNs, routing protocols for WMNs.*

Introduction

WMN is any wireless network where data can be transmitted via mesh networking. First of all we should define what it is WMN. WMN divided into two types: partial mesh network and full mesh network which are illustrated in figure 1. Each node fully interconnects to each other is called as full mesh network, if each node partially interconnects to each other is called as partial mesh network.



The network model is a database model that shows the relationship among the objects. The scheme of network model is viewed as a graph with nodes and connecting links. In the network model, the objects are seen as nodes and the relationships between the objects are depicted as the acts. This network model does not have the hierarchy or lattice; instead, it is replaced with a graph which shows the basic connections between the nodes. The dream of a seamlessly interconnected world would become reality with WMNs.

Partial Mesh Network WMNs permit entire cities to be interconnected by low cost technology. Unlike traditional networks WMNs are based on a small number of wired access points or wireless hotspots to connect users, WMNs provide a network connection spread data between hundred nodes. Each node shares connection across area. The designing of WMNs is simplicity and the network can be provided one-to-one connection and many-to-many connection. Furthermore, data accessing is easy compared to a hierarchical model. WMNs illustrate in graphs with the connections between the nodes. WMNs always have a link that exists between the parent node and **Full Mesh Network** the child node in order to exist the data integrity.

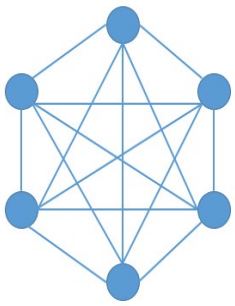


Fig-1

Records in this database model are maintained with pointers, which makes the database more complex in structure and more pointers make the system complex, that is, usage of pointers for each operations like insertion, updating, deleting. Small modifications in the network can be caused changing in the whole application, this makes it structure dependent.

Overview of Wireless Mesh Networks

Over the last few years we have witnessed an increased quest for revolutionizing traditional concepts in wireless communications. Without doubt the most prominent example is the effort towards the extension of the successful paradigm of single wireless hop cellular networks to multi hop wireless communications. WMNs have naturally emerged as a result of this momentum and quickly become an intensive research topic. The efforts for the realization of mesh networks span over a broad set of research activities: from theoretical studies on system capacity to standardization fora such as the IEEE 802.16 standard. WMNs are aiming to fulfil a number of different operational roles, which can vary from rapid deployable, low cost backhaul support to 3G/EEE 802.11 ‘‘x’’ networks to first mile wireless connectivity to the Internet, or even to transient wireless networking. WMNs, can be loosely defined, and this will be our fundamental assumption through-out this chapter, as wireless networks where nodes can act both as clients and routers. We can distinguish two different types of WMNs: client-based and infrastructure-based. The main characteristic of client-based mesh networks is that portable mobile devices participate in the store and forward process. Client based mesh networks operate in a rather autonomous way without the need of a central administration entity. From this perspective, these mesh networks resemble ad hoc networks, which are mainly characterized by energy constraint nodes, i.e., limited battery lifetime, and stochastic mobility. On the other hand, infrastructure-based mesh networks are characterized by nodes that are administered and controlled by a single entity and do not encounter energy constraints.

It is noteworthy that this type of mesh networks flag a different set of research challenges compared to client-based mesh networks. Infrastructure-based mesh networks are characterized by low mobility (or no mobility at all) and by nodes that do not encounter energy constraints.

In that respect, these two types of mesh networks have different operational domains, and in light of these differences the fitness of current proposed solutions for routing, scheduling, and rate control that emerged for ad hoc networks comes into question when applied to infrastructure-based mesh networks.

One approach for multiple access in WMNs is to use contention based (random) access schemes such as ALOHA or different flavors of CSMA. The benefits of random access schemes, such as carrier sense multiple access/collision avoidance (CSMA/CA), is that by using a combination of carrier sensing and back-off algorithms to prevent further conflicts, the nodes can operate in a rather autonomous way.

This is a desirable feature for client-based mesh networks, where resource management procedures should be distributed in nature and quality of service (QoS) support is an add-on rather than a prerequisite feature. For infrastructure-based WMNs that are designed to provide, for example, last-mile broadband Internet access, QoS support, such as throughput and latency, evolves as a rather mandatory requirement. Thus, medium access control (MAC) schemes, such

as TDMA, that allow more deterministic performance guarantees are highly desirable in such scenarios.

Architectures Wireless Mesh Networks

The growing deployment of wireless technology in everyday scenarios actively fosters the evolution of wireless networks into what will be the network infrastructure of our future. Recently, WMNs emerged as a key technology for a variety of new applications that require flexible network support. As an evolution of multi hop mobile ad hoc wireless networks (MANETs), the so-called mesh network configuration maintains the ad hoc communication structure that consists of two architectural levels: mesh routers and mesh clients. Mesh routers have minimal mobility and form the WMN backbone (figure 2). WMNs can serve as indoor or outdoor networks. For example, municipalities would to create their network infrastructure wirelessly or meshes might also serve as outdoor portions of campus networks. As claims that covering areas with WMN offers greater bandwidth at a more affordable cost than 3G cellular networks will be proved to be true, multimedia communications, including video streaming, VoIP, videoconferencing, and online gaming, will start taking full advantage of this new infrastructure. However, each class of applications has a unique set of characteristics that imposes different network requirements to form a viable working solution. Multimedia has been shown to be particularly vulnerable to problems such as bandwidth degradation, network latency, and radio interference with the increasing size and complexity of

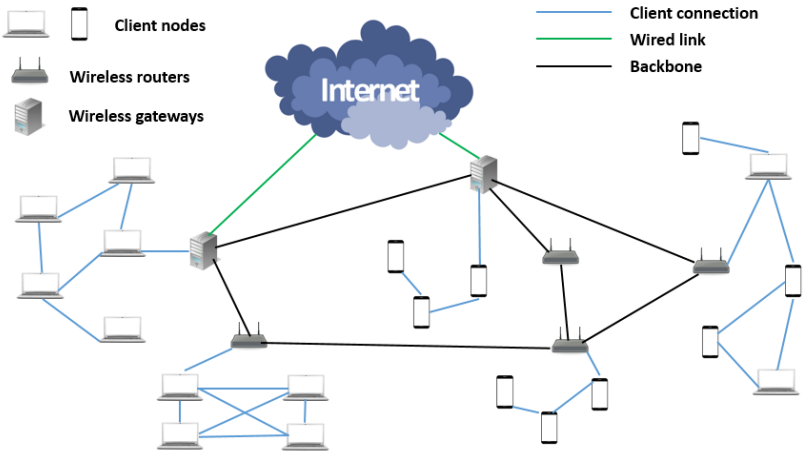


Fig-2. **Architecture of WMN**

multi hop mesh networks. While data flows (web browsing, email delivery, file transfer) may be almost arbitrarily curtailed and still be useful, multimedia communications are more demanding in terms of QoS. In fact, if delay, bandwidth, or packet loss rate are not within a given range, delivering of voice or video data is of no use, e.g., voice communications may lose intelligibility. However, before considering specific multimedia applications and how QoS may be pursued, it is recommended to study and understand the major technical challenges of mesh networking. In fact, the IEEE 802.11 working group is very active in the standardization of new interoperable 802.11-based standards that, in the near future, will provide some interesting capabilities for multimedia communications such as speeds up to 100 Mb/s (and above), QoS support, fast handoff, and mesh functionalities.

Particularly relevant to the mesh networking is the development of the 802.11s standard by the extended service set (ESS) mesh networking task group. Other IEEE 802 working groups are currently involved in the definition of mesh networking extensions to the wireless standards (e.g., 802.15.5, 802.16a, and 802.20). However, with regard to multimedia transmission, and in

particular to real time and interactive services such as videoconferencing systems, very little attention has been devoted to technologies other than 802.11.

Protocols

Wireless mesh networking and mobile ad hoc networking use the same key concept—communication between nodes over multiple wireless hops on a meshed network graph. However, they stress different aspects. Mobile ad hoc networks (MANETs) have an academic background and focus on end user devices, mobility, and ad hoc capabilities. WMNs have a business background and mainly focus on static (often infrastructure) devices, reliability, network capacity, and practical deployment. Nevertheless, one can often find both terms or their variations together in many descriptions or articles on this topic. The core functionality of wireless multi hop ad hoc networking as well as Wireless mesh networks is the routing capability. Routing protocols provide the necessary paths through a WMN, so that the nodes can communicate on good or optimal paths over multiple wireless hops. The routing protocols have to take into account the difficult radio environment with its frequently changing conditions and should support a reliable and efficient communication over the mesh network. Since WMNs share common features with wireless ad hoc networks, the routing protocols developed for MANETs can be applied to WMNs. For example, Microsoft Mesh Networks are built based on Dynamic Source Routing (DSR), and many other companies, e.g., are using Ad hoc On-demand Distance Vector (AODV) routing. Sometimes, the core concepts of existing routing protocols are extended to meet the special requirements of wireless mesh networks, for instance, with radio-aware routing metrics as in the IEEE 802.11s WLAN mesh networking standardization. Despite the availability of several routing protocols for ad hoc networks, the design of routing protocols for WMNs is still an active research area for several reasons.

This section will describe selected routing protocols for wireless multi hop networks as an illustration of the general concepts of routing protocols as well as some special routing protocols for wireless mesh networks.

Ad hoc On-demand Distance Vector Routing Protocol (AODV)

AODV is a very popular routing protocol for MANETs. It is a reactive routing protocol. Routes are set up on demand, and only active routes are maintained. This reduces the routing overhead, but introduces some initial latency due to the on-demand route setup. AODV has been standardized in the IETF as experimental RFC 3561. There are several implementations available, for instance, AODV-UU of Uppsala University. AODV uses a simple request–reply mechanism for the discovery of routes. It can use hello messages for connectivity information and signals link breaks on active routes with error messages. Every routing information has a timeout associated with it as well as a sequence number. The use of sequence numbers allows to detect outdated data, so that only the most current, available routing information is used. This ensures freedom of routing loops and avoids problems known from classical distance vector protocols, such as ‘‘counting to infinity.’’ When a source node *S* wants to send data packets to a destination node *D* but does not have a route to *D* in its routing table, then a route discovery has to be done by *S*. The data packets are buffered during the route discovery. See Figure 3 for an illustration of the route discovery process. The source node S broadcasts a route request (RREQ) throughout the network. In addition to several flags, a RREQ packet contains the hop count, a RREQ identifier, the destination address and destination sequence number, and the

originator address and originator sequence number. The hop count field contains the distance to the originator of the RREQ, the source node *S*. It is the number of hops that the RREQ has traveled so far. The RREQ ID combined with the originator address uniquely identifies a route request. This is used to ensure that a node rebroadcasts an route request only once in order to avoid broadcast storms, even if a node receives the RREQ several times from its neighbors. When a node receives a RREQ packet, it processes as follows:

- The route to the previous hop from which the RREQ packet has been received is created or updated.
- The RREQ ID and the originator address are checked to see whether this RREQ has been already received. If yes, the packet is discarded.
- The hop count is incremented by 1.
- The reverse route to the originator, node *S*, is created or updated.

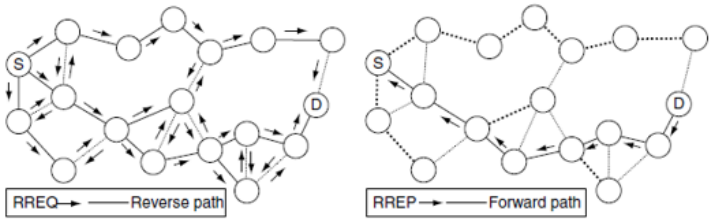


Fig-3. **AODV route discovery: route request (*left*) and route reply (*right*).**

If the node is the requested destination, it generates a route reply (RREP) and sends the RREP packet back to the originator along the created reverse path to the source node *S*.

If the node is not the destination but has a valid path to *D*, it issues a RREP to the source depending on the destination only flag. If intermediate nodes reply to RREQs, it might be the case that the destination will not hear any RREQ, so that it does not have a back route to the source. If the gratuitous RREP flag is set in the RREQ, the replying intermediate node will send a gratuitous RREP to the destination. This sets the path to the originator of the RREQ in the destination. If the node does not generate a RREP, the RREQ is updated and rebroadcast if TTL is _ 1. On receipt of a RREP message, a node will create or update its route to the destination *D*. The hop count is incremented by one, and the updated RREP will be forwarded to the originator of the corresponding RREQ. Eventually, the source node *S* will receive a RREP if there exists a path to the destination. The buffered data packets can now be sent to the destination *D* on the newly discovered path. Connectivity information is provided and maintained by periodically broadcasting routing protocol messages. If a node has not sent a broadcast message, e.g., a RREQ message, within the last hello interval, the node may broadcast a hello message. A hello is actually a RREP with TTLj1 and the node itself as the destination. If a node does not receive any packets from a neighboring node for a defined time, the node considers the link to that neighbor broken. When a link failure has happened, the node before the broken link checks first whether any active route had used this link. If this was not the case, nothing has to be done. On the other hand, if there have been active paths, the node may attempt local repair. It sends out a RREQ to establish a new second half of the path to the destination. The node performing the local repair buffers the data packets while waiting for any route replies. If local repair fails or has not been attempted, the node generates a route error (RERR) message. It contains the addresses and corresponding destination sequence numbers of all active

destinations that have become unreachable because of the link failure. The RERR message is sent to all neighbors that are precursors of the unreachable destinations on this node. A node receiving a RERR invalidates the corresponding entries in its routing table. It removes all destinations that do not have the transmitter of the RERR as next hop from the list of unreachable destinations. If there are precursors to the destinations in this pruned list, the updated RERR message is forwarded to them.

Dynamic Source Routing Protocol (DSR)

DSR is one of the pioneering routing protocols for MANETs. DSR is being standardized in the IETF MANET working group. DSR is a well-known, reactive routing protocol. It computes a route only if one is needed. The route discovery consists of route request and route reply. The route request is broadcast into the wireless network. However, instead of setting the (reverse) paths in the routing tables of the nodes, the route request collects the addresses of the traversed nodes on its way to the destination. Route reply sends this path back to the source where all paths are stored in a route cache. The path, i.e. the list of addresses from the source to the destination, is included in the header of each packet by the source node. Each node forwards a received packet to the next hop based on the list of addresses in the header (source routing). DSR uses RERR messages for the notification of route breaks.

References:

1. *Cass S. Viva Mesh Vegas: The gambling capital antes up for a new mobile broadband technology, IEEE Spectrum Magazine, vol. 53, 2005; 48.*
2. *Akyildiz IF, Xudong Wang, Weilin Wang, Wireless mesh networks: A Survey, Computer Networks, vol. 47, no. 4, 2005; 445-487.*
3. *Bruno R, Conti M, Gregori E. Mesh networks: commodity multihop ad hoc networks: IEEE Communications Magazine, vol. 43, 2005; 123-131.*
4. *Microsoft Mesh Networks. [Internet] Available at: http://research.microsoft.com/mesh/.*