UNIT 5

MESH NETWORKS

1. WHAT IS MESH NETWORK?

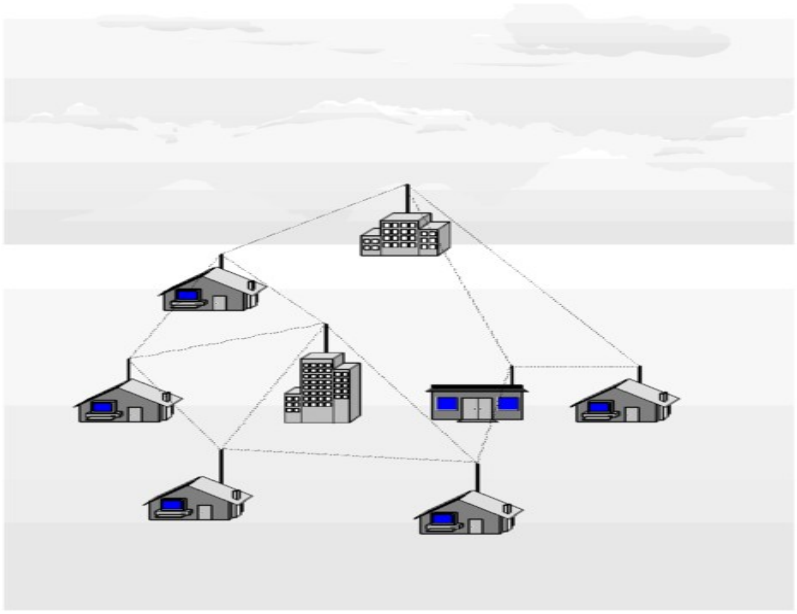
- The term 'wireless mesh networks' describes wireless networks in which **each node can communicate directly with one or more peer nodes.**

- The term 'mesh' originally used to suggest that all nodes were connected to all other nodes, but most modern meshes connect only a sub-set of nodes to each other.

- Nodes are comprised of **mesh routers and mesh clients.**

- Each **node operates not only as a host but also as a router**, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations.

- A WMN is **dynamically self-organized and self-configured,** with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves.



2. NECESSITY FOR MESH NETWORKS

<u>There is a need of the network with following features</u>

- Using **fewer wires** means it costs less to set up a network, particularly for large areas of coverage.
- The more nodes you install, the **bigger and faster** your wireless network becomes.
- **Rely on the same WiFi standards** (802.11a, b and g) already in place for most wireless networks.
- **Convenient** where Ethernet wall connections are lacking -- for instance, in outdoor concert venues, warehouses or transportation settings.

- Useful for **Non-Line-of-Sight** (NLoS) network configurations where wireless signals are intermittently blocked. For example, in an amusement park a Ferris wheel occasionally blocks the signal from a wireless access point. If there are dozens or hundreds of other nodes around, the mesh network will adjust to find a clear signal.
- Networks of **"self configuring;"** the network automatically incorporates a new node into the existing structure without needing any adjustments by a network administrator.
- Networks of **"self healing,"** since the network automatically finds the fastest and most reliable paths to send data, even if nodes are blocked or lose their signal.
- A network configurations allow local networks to **run faster**, because local packets don't have to travel back to a central server.
- Nodes are **easy to install and uninstall,** making the network extremely adaptable and expandable as more or less coverage is needed.

3. ADVANTAGES OF WIRELESS MESH NETWORKS

- Using fewer wires means it **costs less** to set up a network, particularly for large areas of coverage.
- The more nodes you install, the **bigger and faster** your wireless network becomes.

- They **rely on the same WiFi standards** (802.11a, b and g) already in place for most wireless networks.
- They are **convenient** where Ethernet wall connections are lacking -- for instance, in outdoor concert venues, warehouses or transportation settings.
- They are useful for **Non-Line-of-Sight** (NLoS) network configurations where wireless signals are intermittently blocked. For example, in an amusement park a Ferris wheel occasionally blocks the signal from a wireless access point. If there are dozens or hundreds of other nodes around, the mesh network will adjust to find a clear signal.
- Mesh networks are **"self configuring;"** the network automatically incorporates a new node into the existing structure without needing any adjustments by a network administrator.
- Mesh networks are **"self healing,**" since the network automatically finds the fastest and most reliable paths to send data, even if nodes are blocked or lose their signal.
- Wireless mesh configurations allow local networks to **run faster**, because local packets don't have to travel back to a central server.
- Wireless mesh nodes are **easy to install and uninstall,** making the network extremely **adaptable and expandable** as more or less coverage is needed.

4. CHARACTERISTICS OF WIRELESS MESH NETWORKS

- **Multi-hop WMN:**

To provide greater coverage and non-line-of-sight (NLOS) among nodes, the multi-hop function becomes indispensable.

- **Support for ad hoc networking, and capability of self forming, self-healing, and self-organization:**

These properties result in enhanced network performance and gradual growth.

- **Mobility dependence on type of mesh nodes:**

Minimal mobility of mesh routers but mesh clients can be stationary or mobile nodes.

- **Multiple types of network access:**

WMNs can support backhaul access to the Internet and peer-to- peer communications.

- **Dependence of power-consumption constraints on the type of mesh nodes:**

Mesh clients require power efficient protocols in contrast to mesh routers.

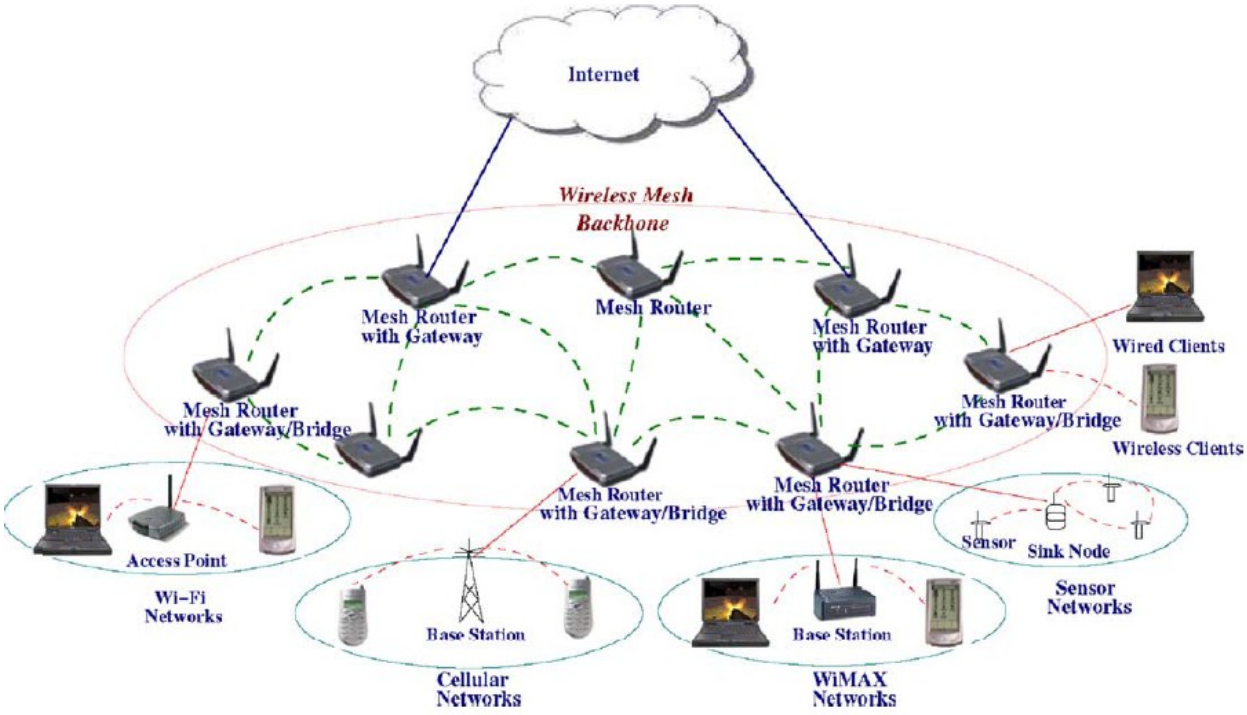
- **Compatibility and interoperability with existing wireless networks:**

WMNs built based on IEEE 802.11 technologies have to be compatible with the IEEE 802.11 standards. Additionaly, such networks must be inter-operable with other types of wireless networks, e.g. WiMAX, ZigBee and cellular networks.

5. ARCHITECTURE OF WMNs.

Three different categories distinguish in the WMNs architecture,
based on the functionality of the nodes.

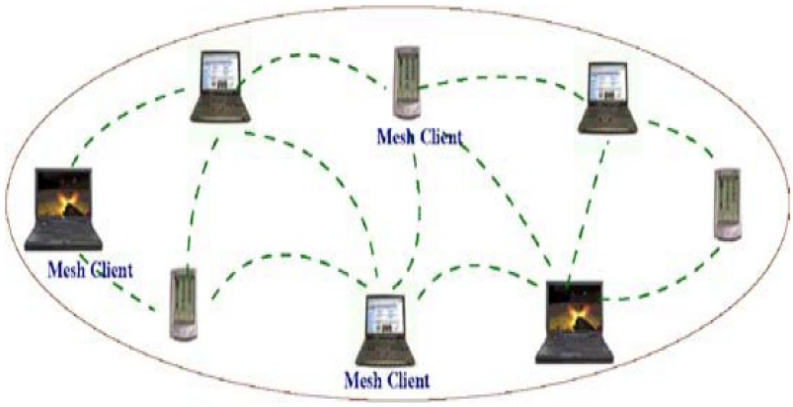
• Infrastructure/backbone WMNs



The above figure shows an infrastructure/backbone WMN. The dashed and solid lines denote wireless and wired connections respectively. As it can be seen in the figure, different kinds of clients connect to the mesh routers that form the infrastructure. The radio technology used by the mesh routers varies significantly. Furthermore, routers apply self-configuring, self-healing links among themselves to form the backbone network.

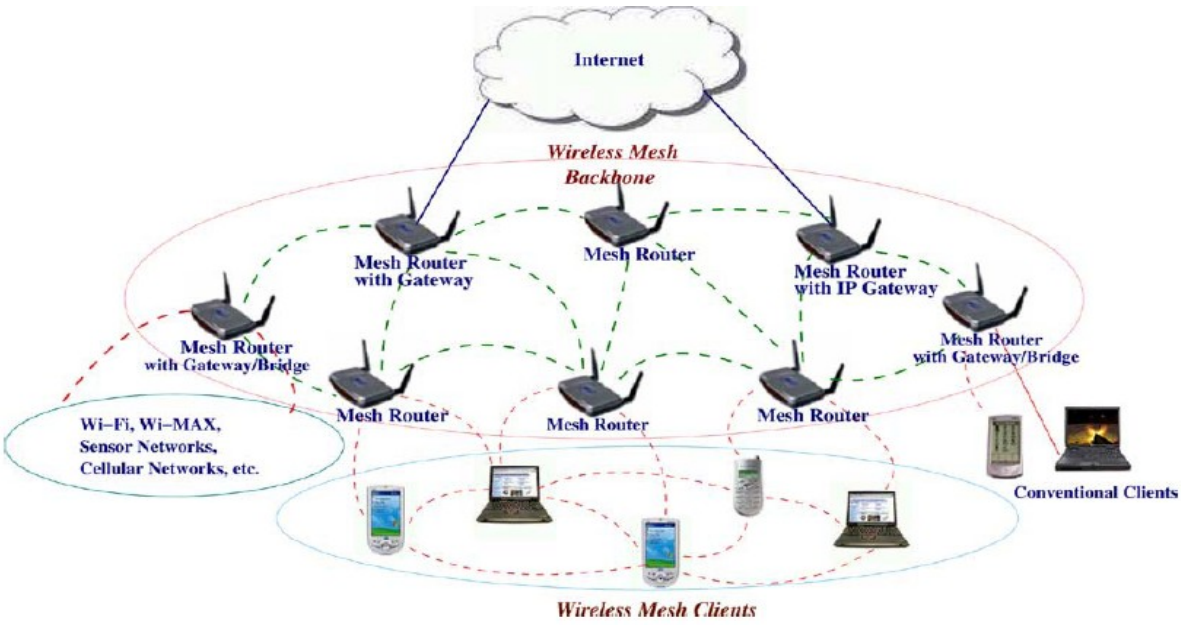
They can also connect to the internet by gateway functions. Conventional clients can connect to the mesh routers either by using the Ethernet interface or by using the same radio technology as the routers.

• Client WMNs



In this type of architecture, no mesh router exists. Instead, conventional devices establish peer-to-peer networks among them to constitute the actuall network performing routing and configuration functions as well as providing end-user applications to customers. There exists one single radio interface among the devices and a packet is forwarded to its destination by hopping through devices.

• Hybrid WMNs



As the name of the architecture denotes, this is the case where the network comprises by both infrastructure and client mesh networks. The clients can access the network by other

clients or by routers providing improved connectivity and coverage within the WMN.

6. 802.11s MAC ENHANCEMENTS

WMN MAC differ from Wireless Networks MACs as follows

- MACs for WMNs are concerned with **more than one hop** communication
- MAC **must be distributed,** needs to be collaborative, and must work for multipoint-to-multipoint communication.

- **Network self-organization** is needed for better collaboration between neighboring nodes and nodes in multi-hop distances.

- **Mobility** affects the performance of MAC.

Improving Existing MAC Protocols

MAC protocols are proposed for multi-hop WMNs by enhancing existing MAC protocols. For example, in an IEEE 802.11 mesh networks, these schemes usually adjust parameters of CSMA/CA, e.g., contention window size, and modify backoff procedures.

However, these solutions only achieve a low end-to-end throughput, because they cannot significantly reduce the probability of contentions among neighboring nodes.

As long as contention occurs frequently, whichever method is taken to modify backoff or contention resolution procedures, the end-to-end throughput will still be significantly reduced due to the accumulating effect on the multi-hop path.

The existing 802.11 MAC layer is being enhanced for

- **Supporting QoS:**

  - EDCA(Enhanced Distributed Channel Access) specified in 802.11e, as the 802.11s' basic operation mechanism
  - Other features of 802.11e, like HCCA, are not considered.

EDCA is a mandatory mechanism in 802.11e that is reused in 802.11s to provide prioritized QoS services.

EDCA

Enhanced Distributed Channel Access is an extension of Distributed Coordination Function (DCF). Thus, DCF is the basis for EDCA. QoS stations (QSTAs) access the medium using 8 different user priorities (UPs). This means that packets sent by the QSTAs are assigned a priority value, before entering the MAC. These packets are then mapped to the four first-in first-out (FIFO) queues,called access categories (ACs) implemented in EDCA. For each AC, an enhanced variant of the DCF, namely the enhanced distributed channel access function (EDCAF), contends for TXOPs using a set of EDCA parameters.

Transmission opportunity (TXOP) is defined as the interval of time when a particular QSTA has the right to initiate transmission. Eack AC behaves like a virtual station: it contends for medium access starting its backoff timer after sensing the medium idle after AIFS, (AIFS being the corresponding DIFS in DCF). The rule that applies is that the AC with the lowest AIFS has the higher priority. The different parameters are used to give a low-priority class a longer waiting time.

MDA

In Mesh Deterministic Access (MDA) scheme, involving MPs have to support sychronization. MDA sets up time periods, called MDAOPs, to prevent MPs of initiating transmission sequences in case they interfere with each others transmissions or receptions. MPs that set up MDAOPs access the medium by using the MDA access parameters CWMin, CWMax, and AIFSN within these periods.

A Mesh DTIM interval comprises of MDAOPs, such an interval is set up between the MDAOP owner and the addressing MP. After the MDAOP is set up:

• The MDAOP owner uses CSMA/CA and backoff to obtain a TXOP using the MDACWmin, MDACWmax, and MDAIFSN parameters. The ranges of values of the parameters are identical to those used in EDCA.

• Both the MDAOP owner and the addressed MP advertise the MDAOP. Except the MDAOP owner, all other MPs should not initiate transmissions during the TXOP initiated in the MDAOP.

A sender MP has the ability to establish a set of MDAOPs each identified by a unique ID called the MDAOP Set ID. Such a set id has to be unique for the sending MP, so that the MDAOP

set ID and the senders MAC address uniquely identify an MDAOP set in the mesh. A MDAOP Set ID can also handle set up and teardown of the the entire set of MDAOPs in an MDAOP set.

TXOPs also exist in MDA but since it is obtained by a MP in a MDAOP, it is called MDA TXOP. Such an TXOP is required to end within the MDAOP it origianlly was obtained. Neighborhood MDAOP times for a MP are those TXRX
times that are advertised by neighboring MPs, forming a set of MDAOPs currently used in the neighborhood. Thus, a sender cannot set up new MDAOPs within these times. Neighbor MDAOP interfering times for a MP in relation to another MP are the times when the former cannot set up MDAOPs with the latter. Thus, creating MDAOPs within these times can and will result in interference.

The MDA access fraction, at a MP, is defined as the ratio of the total duration of its Neighborhood MDAOP Times"in a Mesh DTIM interval to the duration of the Mesh DTIM interval. It exists to make sure that a new MDAOP set does not cause the MAF of another MP to exceed a MAF limit. If the limit is exceeded, the MDAOP request should be refused.

An MDA Manager exists to allow end-to-end flows using MDA features
and is responsible for

- Path computation.
- Invoking MDAOP Setup Procedure on node along the path.

The MDA Manager can make path computation in the following two different ways:

- Using Dijkstra algorithm.

• Using Ford algorithm.

- **Improving the network capacity:**
  - The usage of multiple channels and multiple radios
  - Efficient handling of the two different kinds of traffic (BSS traffic & Forwarding mesh traffic)
  - Intra-mesh congestion control
  - Mesh coordinated channel access
  - Handling BSS and mesh traffic by Mesh AP
- **Giving priority to mesh traffic may starve STAs**
- **Giving priority to STAs might waste resource utilized by mesh traffic**
- **Advanced solutions: separate radio for mesh and BSS traffic**
  - Intra-mesh congestion control
- **A simple hop-by-hop congestion control implemented at each MP**
- **Local congestion monitoring, Congestion control signaling, Local rate control**

- **Mesh Coordinated Channel Access (MCCA)**

- **Optional scheme based on the reservation of contention free time slots**

- **Lower contention (more deterministic) mechanism for improved QoS for periodic flows**

    - Mobility is of little concern (do not support seamless handover).
    - No mechanism for multi-channel operation

- **One proposal called "CCF (Common Channel Framework) was adopted in the early version of the draft (before draft 1.0), but removed from the draft.**

- **Limitations caused by the EDCA**

    - Performance limitations in multi-hop environments
    - End-to-end QoS limitations

- **More reliable and stable metric for link quality measurement and routing.**

- **Better solutions for power management.**

- **More robust approaches than its current security solution inherited from 802.11i, in**

terms of routing security or end-to-end security.

MAC Improvements

Cross-layer design with advanced physical layer techniques

MACs based on Directional Antennas

Eliminate exposed nodes if antenna beam is assumed to be perfect. Due to the directional transmission, more hidden nodes are produced. Also face other difficulties such as cost, system complexity, and practicality of fast steerable directional antennas.

Proposing Innovative MAC Protocols:

Determined by their poor scalability in an ad hoc multi-hop network, random access protocols such as CSMA/CA are not an efficient solution. Thus, revisiting the design of MAC protocols based on TDMA or CDMA is indispensable. To date, few TDMA or CDMA MAC protocols are available for WMNs, probably because of two factors:

- The complexity and cost of developing a distributed and cooperative MAC with TDMA or CDMA.

- The compatibility of TDMA (or CDMA) MAC with existing MAC

protocols.

MACs with Power Control

They reduce exposed nodes, especially in a dense network, using low transmission power, and thus, improve the spectrum spatial reuse factor in WMNs. However, hidden nodes may become worse because lower transmission power level reduces the possibility of detecting a potential interfering node.

For example, in IEEE 802.16, the original MAC protocol is a centralized TDMA scheme, but a distributed TDMA MAC for IEEE 802.16 mesh is still missing.

In IEEE 802.11 WMNs, how to design a distributed TDMA MAC protocol overlaying CSMA/CA is an interesting but a challenging problem.

Multi-Channel Single-Transceiver MAC:

If cost and compatibility are the concern, one transceiver on a radio is a preferred hardware platform. Since only one transceiver is available, only one channel is active at a time in each network node. However, different nodes may operate on different channels simultaneously.

To coordinate transmissions between network nodes under this situation, protocols such as the multi-channel MAC and the seed-slotted channel hopping (SSCH) scheme are needed. SSCH is actually a virtual MAC protocol, since it works on top of IEEE 802.11 MAC and does not need changes in the IEEE 802.11 MAC.

Multi-Channel Multi-Transceiver MACs

A radio includes multiple parallel RF front-end chips and baseband processing modules to support several simultaneous channels. On top of the physical layer, only one MAC layer module is needed to coordinate the functions of multiple channels.

To date, no multi-channel multi-transceiver MAC protocol has been proposed for WMNs.

Multi-Radio MACs

The network node has multiple radios each with its own MAC and physical layers. Communications in these radios are totally independent. Thus, a virtual MAC protocol such as the multi-radio unification protocol (MUP) is required on top of MAC to coordinate communications in all channels. In fact, one radio can have multiple channels in this case. However, for simplicity of design and application, a single fixed channel is usually applied in each radio.

Scalable Single-Channel MACs:

The scalability issue in multi-hop ad hoc networks has not been fully solved yet. Most of existing MAC protocols only solve partial problems of the overall issue, but raise other problems. To make the MAC protocol really scalable, new distributed and collaborative schemes must be proposed to ensure that the network performance (e.g., throughput and even QoS parameters such as delay and delay jitter) will not degrade as the network size increases.

Scalable Multi-Channel MACs

Multi-channel MAC protocols for radios with multiple transceivers have not been thoroughly explored, possibly due to the relatively high cost of such radios. However, as the cost goes down, a multi-channel multi-transceiver MAC will be a rather promising solution for WMNs.

It is obvious that a multi-channel MAC protocol can achieve higher throughput than a single-channel MAC. However, to really achieve spectrum efficiency and improve the per-channel throughput, the scalable MAC protocol needs to consider the overall performance improvement in multiple channels.

Thus, developing a scalable multi-channel MAC is a more challenging task than a single-channel MAC.

7. IEEE 802.11s ARCHITECTURE

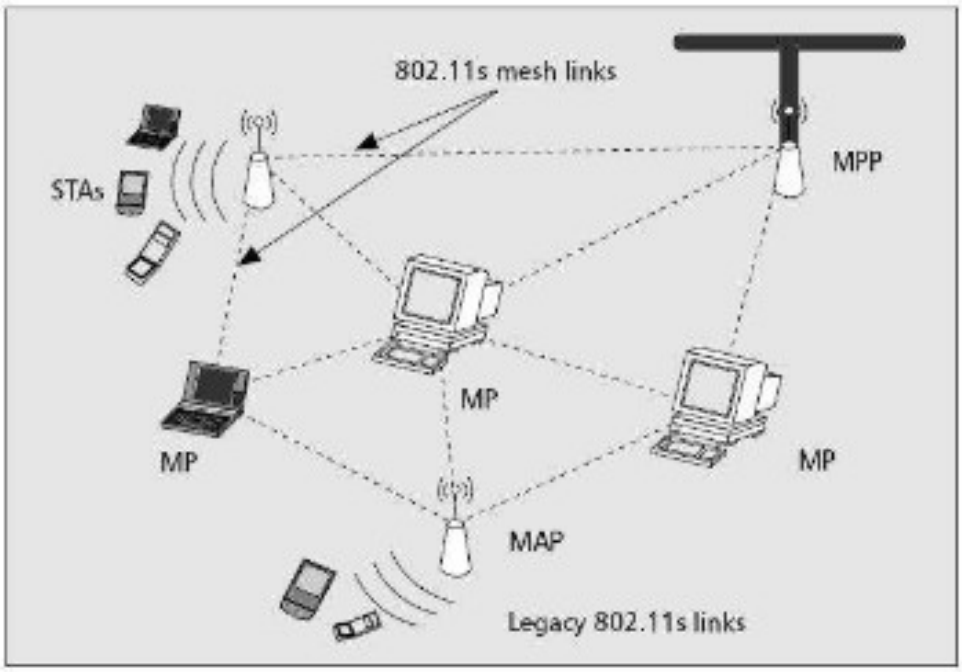
802.11s is an amendment being developed to the IEEE 802.11 WLAN (Wireless Local Area Networks) standard.

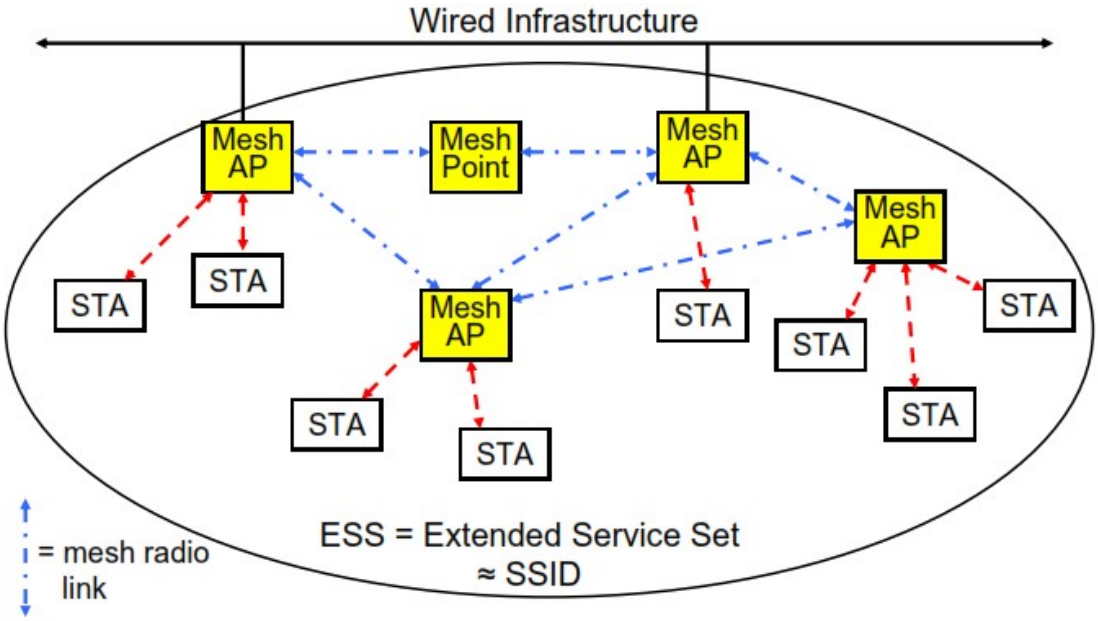
802.11s Scope

• **802.11s WLAN Mesh Networking -** Integrates mesh networking services and protocols with 802.11 at the MAC Layer

- **Primary Scope:**
    - Amendment to IEEE 802.11 to create a Wireless Distribution System with automatic topology learning and wireless path configuration.
    - Small/medium mesh networks (~32 forwarding nodes) – can be larger.
    - Dynamic, *radio-aware* path selection in the mesh, enabling data delivery on single-hop and multi-hop paths (unicast and broadcast/multicast).
    - Extensible to allow support for diverse applications and future innovation.
    - Use 802.11i security or an extension thereof.
    - Compatible with higher layer protocols (broadcast LAN metaphor).

The **network architecture** is depicted in the following figures.





Device Classes in a WLAN Mesh Network

• **Mesh Point (MP):** establishes peer links with MP neighbors, full participant in WLAN Mesh services. Light Weight MP participates only in 1-hop communication with immediate neighbors (routing=NULL).

• **Mesh AP (MAP):** functionality of a MP, collocated with AP which provides BSS services to support communication with STAs.

• **Mesh Portal (MPP):** point at which MSDUs exit and enter a WLAN Mesh (relies on higher layer bridging functions).

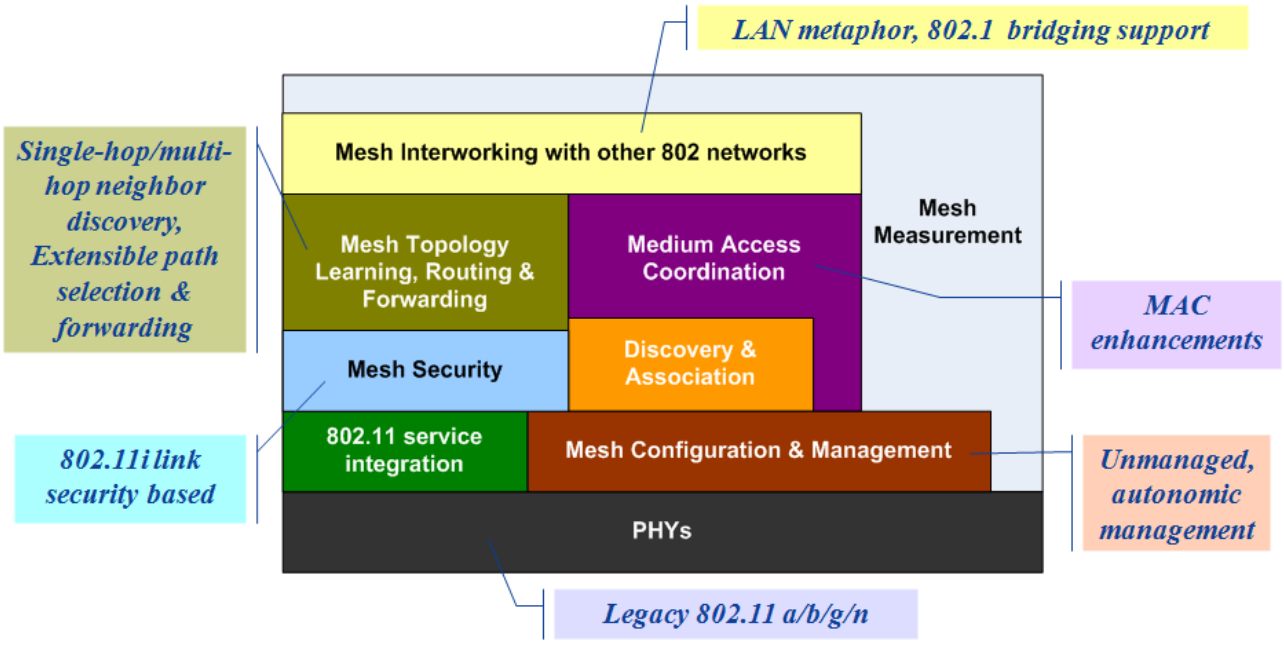
• **Station (STA):** outside of the WLAN Mesh, connected via Mesh AP.

The 802.11 defines an extended service set (ESS), usually refered to as a mesh network. Every IEEE 802.11-based entity (AP or STA) that fully or partially supports mesh functionality is refered to as a mesh point (MP). Minimal MP operations include neighbor discovery, channel selection, and forming associations with neighbors. A WDS is formed by MPs and mesh links that

connect the MPs. This way, the ESS is distinguished from the BSS, defined in the legacy IEEE 802.11. MAPs are specific MPs but can act as APs as well.

MPPs is another type of MPs that has the ability of interconnecting other WMS with the network it belongs to. Furthermore, it can act as a bridge/gateway of the mesh network and other networks in the DS. Such a WMN is uniquely identified by a mesh ID assigned to every MP to represent an ESS.

Medium Access Coordination Function



The Medium Coordination Function (MCF) components are shown in the above figure. The sublayer is built on top of the PHY layer where no modifications have been made. The 802.11s MAC sublayer is an amendment to IEEE 802.11 to create a WDS.

The most important parts of MFC are,

Mesh Topology Learning, Routing and Forwarding

Focused on peer-to-peer discovery of MPs, this service set (SS) enables automatic topology learning, establishes links and forms a dynamic data delivery path across MPs.

- Topology discovery and formation:

  A new candidate node initially gathers information from neighboring nodes either by active scaning (i.e. sending probe messages) or by passive listening (i.e. by receiving periodic beacons). Finally, two peers form a partial or a full mesh topology by associating with each other.

- Path selection protocol:

  Formally, a L2 path selection protocol is used to handle unicast and broadcast/multicast data delivery. On the other hand, MPs might be mobile or nonmobile and thus a hybrid routing protocol supporting both proactive and on-demand schemes is more suitable for such a network. Thus, the hybrid scheme uses the ad hoc on-demand vector (AODV) and the optimized link state routing (OLSR) to reach the goal. To make the routing prototcols more robust against link failures, radio aware metrics are proposed.

- Forwarding scheme:

  The traffic in a WMN consists of 4-address data frames. When a MP receives such frames, it checks for the frame authenticity and the destination MAC address before forwarding. In the MAP arrive the 3-address frame which is converted to a 4-address format and then it is

forwarded to its destination. The support of forwarding multicast and broadcast traffic is also supported.

Medium Access Coordination

The proposal is to use the enchanced distributed channel access (EDCA) mechanism as medium access coordination which is the re-use of previous MAC encahncements, i.e. 802.11e. The MAC mechanisms support congestion control, power saving, synchronization and beacon collision avoidance. The proposed mechanisms shall make it possible to enable multiple channel operations in multiradio or single radio as well as mixed environments. Furthermore, there must be compatibility with legacy devices.

Optional MAC enchancements include Mesh Deterministic Access (MDA) that is a reservation-based deterministic mechanism, Common Channel Framework (CCF) that is a multi-channel operation mechanism, Intra-mesh Congestion Control and power management.

Mesh Configuration and Management

Since the deployment of self-configuring paths and links can be unmanaged, it is required the use of autonomic management modules. The purpose of management is to ensure a free of problems network operation. A mesh point that may fail does not effect the overall network performance but it has to be managed anyway.

Use Cases are detailed below:

- **Residential Case**

In this model, the primary purposes for the mesh network are to create low-cost, easily deployable, high performance wireless coverage throughout the digital home. The mesh network is intended to eliminate RF dead-spots and areas of low-quality coverage. High bandwidth applications tend to be used but also simple ones, e.g. video streaming and wireless printers.

- **Office Case**

The objective in the office case is to create low-cost, easily deployable wireless networks that provide reliable coverage and performance. A wireless mesh LAN becomes useful in areas where Ethernet cabling does not exist or is cost prohibitive. Companies reduce their costs in association with cable and time of installation. Furthermore, they can benefit also from increase in employee productivity through expanded connectivity to key network resources.

- **Campus / Comamunity / Public Access Case**

Mesh networks can in this case provide connectivity over large geographic areas in low cost, higher bandwidth internet access in contrast to the traditional methods and location based services for information and safety purposes.

- **Public Safety Case**

Access to emergency and municipal safety personnel such as fire, police, and hospital is important if a corresponding incident occurs. The network can be used for video surveillance, tracking emergency workers with biosensors,

voice and data communication between emergency personnel and so on.

Mesh Security Considerations

- **Functions in the scope**
  Transport level security

- **Functions out of the scope**
  - Internal routing
  - External routing
  - Forwarding
  - Current technology is not mature enough to address all vulnerabilities from routing and forwarding

Transport Security

Prevent unauthorized devices from directly sending and receiving traffic via the mesh. It protects unicast traffic between neighbor MPs and protects broadcast traffic between neighbor MPs.

It is required to mutually authenticate neighbor MPs and to generate and manage session keys and broadcast keys. Data confidentiality over a link needs to be maintained. It is essential to detect message forgeries and replays received on a link.

Authentication and Initial Key Management

Basic approach is to re-use 802.11i/802.1X facilitates implementation and allows other AKM schemes. 802.1X is widely used and is suitable for many mesh scenarios. It can be replaced with small scale alternatives if required. It Provides a basis for secure key distribution (PMK).In a mesh, PMK is treated as token of authorization for a MP to join the mesh and authorized to send and receive messages to/from mesh neighbours.

Discovery and Role Negotiation

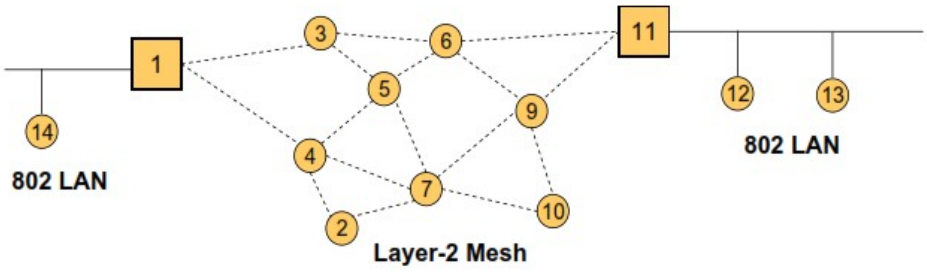
Discovery

This service implies to discover the available mesh for joining and what Authenticated Key Management (AKM) Protocol is being used and to ensure the availability of Unicast and Multicast Ciphersuites.

Negotiation

This service enables parties to agree on the security roles and security policy to use with a peer link, Who's the authenticator, who's the supplicant? and agree on which of those options enabled to use.

802.11s Interworking Approach



Support for connecting an 802.11s mesh to an 802.1D bridged LAN

- Broadcast LAN (transparent forwarding)
- Overhearing of packets (bridge learning)
- Support for bridge-to-bridge communications (e.g. allowing Mesh Portal devices to participate in STP)

Interworking: MP view

1. Determine if the destination is inside or outside of the Mesh

a. Leverage layer-2 mesh path discovery

2. For a destination inside the Mesh,

a. Use layer-2 mesh path discovery/forwarding

3. For a destination outside the Mesh,

a. Identify the “right” portal, and deliver packets via unicast

b. If not known, deliver to all mesh portals

Opportunistic Networks

In many MANET application environments, nodes form a Disconnected networks due to nodal mobility, node sparseness, lossy link of signal attenuation or shut-down the transmission to conserve energy and etc.

Traditional MANET and Internet routing/forwarding techniques are not available because they implicitly assume that the network, even if sparse, is connected (or can be made by e.g. tuning transmitting powers) and an end-to-end path always exists between any source-destination.

- Constitute the category of ad hoc networks where diverse systems, not originally employed as components, join in dynamically to exploit the resources of separate networks according to the needs of specific application tasks.

- Communication Opportunities (contact) are intermittent.

- Network is partitioned & No continuous end-to-end path

- Applications

    Delay Tolerant Networks (DTN)
    Pocket Switched Networks (PSN)
    Socio-aware Community Networks

If different links come up and down, over time, due to occasional partial-connectivity or node mobility, the sequence of connectivity graphs over a time interval are overlapped, then an end-to-end path might exist.

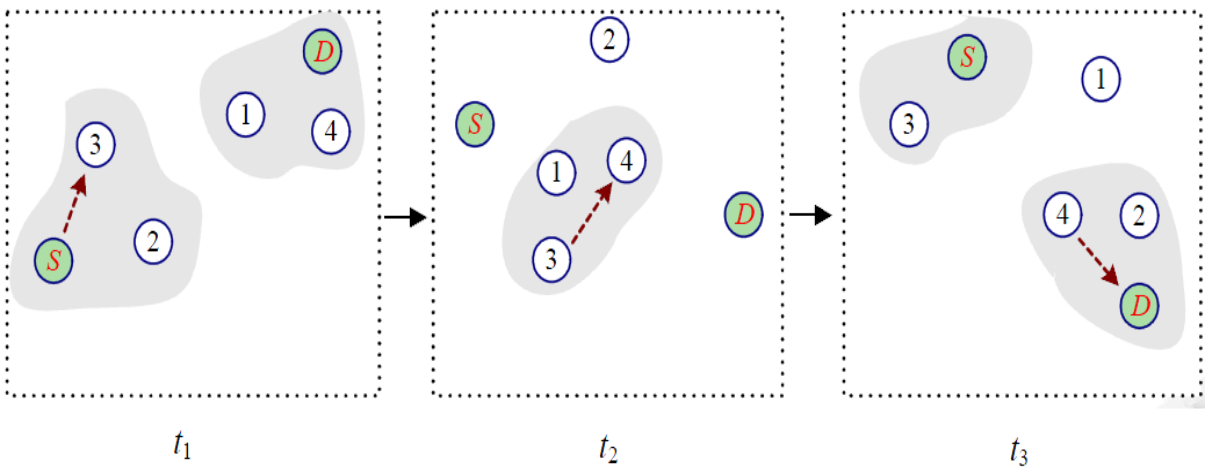
This implies that a message could be sent over an existing link, get buffered at the next hop until the next link in the path comes up, and so on and so forth, until it reaches the final destination

- Store-Carry-Forward routing pattern.

This imposes a new model for routing, which consists of independent, local forwarding decisions, based on the current connectivity information and possible prediction of future connectivity.

If a message can't be delivered immediately, the best carriers are the those having the highest chance of successful delivery.

Opportunistic Networks: Illustration



Opportunistic Routing

Routing category:

- Context information based
- Geographical information based
- Signal strength based
- Infrastructure based
- Hybrid strategy

OppNet Routing: Context information

The context in which the users communicate like:

- Node mobility information
- History of node behavior
- Networks connectivity

Therefore, given context information about the destination, suitable forwarders could be chosen based on:

- The probability of contact with other users
- The probability of visiting particular places

Context-aware routing classification

1. Context-oblivious

- Basically exploit some form of flooding
- Good latency
- High overload

2. Partially Context-aware

Exploit some particular piece of context information (e.g. node mobility) to optimize the forwarding task

3. Fully context-aware

Not only exploit context information to optimize routing, but also provide general mechanisms to handle and use context information

1. Context-oblivious Routing Protocols

- Flooding-based
- Message should be disseminated as widely as possible
- The only solution when no context information is available
- High Overload

To limit overload, possible techniques is to control flooding by

- Limiting the number of copies
- Limiting the number of hops

May suffer high contention and potentially lead to networks congestion

Examples

- Epidemic routing
- Spray & Wait
- Networking Coding

Context-oblivious Protocols: Epidemic

a) Epidemic Routing

- When two nodes meet, exchange summary vectors which contain with compact representation of the messages currently stored in their local buffers.
- Then, each node requests from the other the message which it is currently missing
- Good delivery rate and latency
- Exhaustion of resources, storage management strategy is important

Context-oblivious Protocols: Spray & Wait

b) Spray & Wait

Two phases: Spray phase and Wait phase

Spray phase: L copies of the same message are spread over the networks both by the source node and those nodes that have first received the message from the source itself

Wait phase: each node holding a copy of the message does nothing but simply store its copy and wait to eventually deliver it to the destination when it comes insides the range

Spray can be performed in multiple ways

L can be chosen based on a target average delay

2. Partially Context-aware Protocols

Exploit some piece of context information to optimize forwarding e.g. Encounter information / mobility information

Examples

- Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET)
- Spray & Focus
- Bubble Rap

Partially Context-aware Protocols: PROPHET

a) PROPHET

Evolution of Epidemic: during a contact, nodes also exchange their Delivery Predictability (DP) to destinations of the message they store in their buffers

Messages are requested only if DP is higher than that of the node currently storing the message

DP is the probability for a node to encounter certain destination

Increases when the node meets the destination

Decreases (according to an ageing function) between meetings

Context information used by PROPHET is the “frequency-of-meeting” between nodes.

Partially Context-aware Protocols

b) Spray & Focus

Improve the Wait phase of Spray & Wait, in Focus phase, each relay can forward its copy to a potentially more appropriate relay node independently, using a carefully designed utility-based scheme.

c) Bubble Rap

Automatically infer the parameters of the underlying social structure Dynamically identifies users' communities, ranks the nodes "sociability" (measured as the number of links) within each community

- Each node has a global ranking (across the whole system) and local ranking both depends on the sociability information.
- Exploit the structure property to select forwarding path
- Context information is the "Popularity" or "Sociability" in the social networks

3. Fully Context-aware Protocols

Provide general mechanisms to handle and use context information

More general than Partial Context-Aware:

Works with any context information
Can be customized for the specific environment

Examples

- PROPICMAN (Probabilistic Routing Protocol for Intermittently Connected Mobile Ad hoc Networks)
- HiBOp (History-Based Opportunistic routing)
- CAR (Context-aware Adaptive Routing)

Fully Context-aware Protocols: PROPICMAN

Exploit the context information of nodes to select the best next-hop candidate (e.g. work place, city, street, name, hobby, etc.)

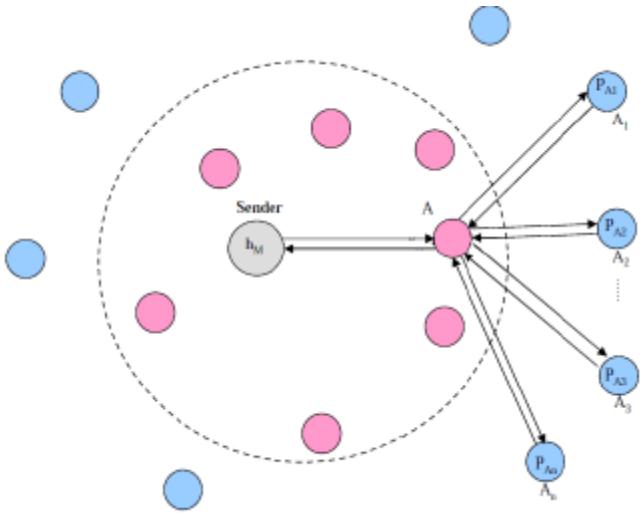
>Each node has a common Node Profile with evidence/value pairs, evidences have different weights

Evidence Name(E)	Value(V)
Work Place	IAM
City	Bern

Source node knows some information about destination D's profile & build a message header h_M which is the concatenation of all the hashed function of evidence/value pair like:

$$h_M = \underset{i=1}{\overset{n}{Concatenation}}(H(E_{D_i}, V_{D_i}), MAC_S, SN_M)$$

a) PROPICMAN



S sends h_M to every neighbor node, without the original message content.

>Neighbor A compares the header pairs of evidence/value in h_M with its own hashed value.
>For each matching element, A gets the weight of that evidence. From all the matching elements, the Delivery Probability of A is:

$$P_A = \frac{\sum Matched(W_i)}{\sum W_{M_i}}$$

b) Fully Context-aware Protocols: CAR

Nodes are divided into partitions

- Nodes inside the same partition are connected by an underlying proactive MANET routing protocol (e.g. DSDV), each node has its own routing table.
- The nodes located in the other partitions of the network are not reachable through classical routing protocol.

Focus on expanding the classical routing table to support forwarding across intermittently-connected ad hoc networks by adding a “Delivery Probability” item, to each “Destination -Best Forwarder” entry.

Each node produces its own delivery probability towards each known destination.

Choice of the best carriers based on the evaluation of the Multiple-attributes utility-based framework.

CAR

Context information consists of
Logical connectivity of networks:

- The rate of connectivity change
- The degree of mobility

Device information

- Residual battery life
- Available memory

Process

- Time Series Analysis to predict the evolution of the network scenarios (future value of context attributes).
- Multi-attribute utility theory to produce a composition of all the estimated values as a utility function.

SELF CONFIGURATION AND AUTO CONFIGURATION

The performance of any network is a critical factor that needs to be considered before it gets accepted and deployed at large scale for various commercial applications. In the context of WMNs, the issues which affect their performance include the following:

• ***Distributed MAC & Multihop Communication:*** Because of the 'decentralized' nature of mesh networks, the MAC function should be accomplished in a distributed manner i.e. to establish multi-point to multi-point links between the mesh nodes in the absence of centralized controller. Moreover, the MAC protocol for WMNs needs to have multihop communications at the core of its design. Several distributed channel assignment and MAC protocols have been proposed which improve the throughput in multi-hop paths. However they are still far from being optimum solutions to be exploited by the network operator for commercial deployments. Apart from these, one needs to properly identify the issues related to the spectral efficiency of both high frequency and low frequency mesh systems. Proper characterization for the mesh capacity constraints is very important in determining the practical utility of mesh networks and its enabling technologies.

• ***Mesh Routing:*** Mesh networking requires each node to share route information with other nodes. This functionality should be assured by the mesh routing protocol. Some efforts have been initiated to adapt the ad-hoc routing protocols for WMNs. However ad-hoc routing protocols lack various important performance factors such as scalability, fault tolerance, QoS metrics (fairness), load balancing, and lack of cross layer interaction. In addition, certain areas such as mobility and power management have totally different requirements in ad-hoc networks and WMNs. This makes ad-hoc routing solutions not particularly suitable for WMNs.

• ***Application and Service Perspective:*** Every application and service has its own inherent characteristics which makes it perform well on one platform and not on

another. Due to the distributed multihop features of mesh networks and the non significant support from the lower layers to assure certain quality of service support for the application layer, there is a pressing need to adapt the existing applications to WMN architecture.

Interoperability and Integration: Due to the emergence and rapid growth of heterogeneous wireless access technologies such as WiFi, WiMAX, UWB, various cellular systems etc., interoperability and integration are a major concern for future wireless systems. While WMNs can probably serve as a unifying technology for all these disparate systems, more research still needs to be performed to ensure that seamless service can be offered to users irrespective of access technology.

OVERVIEW OF WMN OPERATION

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. Typically, a mesh network is reliable and offers redundancy since links are typically "any to- any". When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks are technology-agnostic i.e. they can be implemented with various wireless technology including 802.11, 802.16, cellular technologies.

ASSUMPTIONS

Based on the information above, some key assumptions were made while developing this framework.

1. Internet access occurs only via the mesh infrastructure nodes. These nodes are largely stationary or move very infrequently.

2. The subscription module (token or smartcard) used in the WMN devices is tamper-resistant. Any attempts to modify its contents results in a network notification

and invalidation of the token. This Token contains the subscriber's ID, ESSID, assigned wireless channels (where applicable e.g. in a regulated environment), and PKI private key.

3. IP address assignment is adaptable based on the network the node is allowed to join. This differs from most other projects that concentrate on configuration and not deployment i.e. it is implicitly assumed that there are no competing networks. This is also critical to our objective to allow commodity hardware to be used for different networks. The key difference between nodes belonging to different networks would be subscription-based credentials stored on a module

or some form of smart card.

4. It is designed to be routing-protocol agnostic. There is no need to design a routing protocol specifically for the network. Any routing protocol (proactive or reactive) should be able to work within the mesh. The discovery, boot-strapping and registration process all serve to aid Layer 3 reachability i.e. the topology built during network discovery should be useful to any routing protocol.

5. The nodes used in the WMN are multi-channel, multi-radio nodes; Data and control packets can be sent out via either interface. Channels are bound to links and not nodes (edges, not vertices). Channel assignment seeks to assign more non-overlapping channels to connections closer to the root. The number of channels assigned by node is limited to the number of radios present. Channel re-use should be utilized wherever possible. The following assumptions are made:

_ There is a control radio for management

_ The channel assignment is provided for self-configuration

_ The network has a known good connection state that can be used for fallback

6. The composite metric used to determine the network's topology is unique. It is calculated in a distributed fashion, adaptive and is weighted to give preference to link reliability (interference, Signal-to-Noise ratio), channel capacity (bandwidth) and

queue occupancy which helps ensure intrinsic topology fairness. Queue occupancy should a weighted average calculated over a sample period.

7. Self-healing should not trigger a re-configuration of the topology tree. It should use alternate links discovered during the discovery, bootstrapping and registration process. This will ensure long-term stability of the network's topology. This is done over the common signaling channel. To prevent long term unfairness, in the event of a failure, a node should try to discover another parent node after a certain period of time. It should do this by scanning for beacons promiscuously. In the event that a node has only one link (i.e. no standby connections), it should automatically start the membership and initialization phase again.

8. When the tree needs to be recalculated due to a long-term change in physical connectivity, it should be done as locally as possible i.e. it should occur in the "leaves" of the tree first (children nodes) before spreading to the branches (delegated parent nodes) and maybe the root (parent nodes). This takes advantage of the fact that nodes closer to the root (the 'branches') are more stable than edge nodes (the 'leaves'). This is due to the fact that those nodes are likely to be installed by the provider which means that their connectivity is better constructed with a less likely chance of failure.

9. The algorithm is both distributed and centralized. The discovery, boot-strapping and registration process are distributed while the centralized portion consists of agents running on the nodes reporting to a centralized manager with status on various network variables as well as configuration of parameters such as IP addressing and QoS settings.

10. It is assumed that not all nodes are cooperative. While we believe our scheme can work for community-based WMNs, it is developed using a service provider oriented concept where identity of the subscriber is essential to the delivery of service.

NODE INITIALIZATION

There are two general approaches that have been used for the development of MAC layer protocols in WMNs:

Single-channel MAC: The single-channel MAC is the most pervasively deployed link layer scheme for wireless networks. 802.11 WLANs are based on the CSMA/CA protocol (Carrier Sense Multiple Access With Collision Avoidance). Protocols such as those found in are enhancements of the CSMA/CA protocol. Schemes in this category typically adjust parameters of CSMA/CA such as contention window size and modify backoff procedures. Even though they may improve throughput for one-hop communications, their performance suffers in WMNs as they usually yield a low end-to-end throughput, because they cannot significantly reduce the probability of contentions among neighboring nodes. The benefits of any scheme using this approach are likely to diminish in environments where links have frequent contention and packet

collision.

Cross-layer design leveraging physical layer techniques: Two major schemes exist in this category: MAC based on directional antenna and MAC with power control. The first scheme relies heavily on advanced antenna technology to ensure that communication between nodes is as focused as possible to reduce interference. However, its practical use is questionable as it is highly unlikely that the antenna's beam will be perfect 100% of the time. Cost and complexity or hardware is also an issue. The second set of schemes utilizes power control to reduce interference. This can help reduce exposed nodes problem, especially in a dense network, thereby improving spatial reuse in the network. However, hidden nodes still exist and may become worse because lower transmission power level reduces the possibility of detecting a potential interfering node.

Multi-channel MAC: A multi-channel MAC can be implemented on several different hardware platforms, which also impacts the design of the MAC. The design can be based on a single transceiver or multiple transceivers. With a single transceiver, only one channel can be active at a time. Multiple nodes may operate on different channels to help boost network capacity. To coordinate transmissions between network nodes under this situation, protocols such as the multi-channel MAC and the seed-slotted channel hopping (SSCH) scheme are needed.

Multi-radio MAC: In this scenario a network node has multiple radios each with its own MAC and physical layers. Communications in these radios are totally independent. Thus, a virtual MAC protocol such as the multi-radio unification protocol (MUP) or Microsoft's Mesh Connectivity Layer is required on top of MAC to coordinate communications in all radio links and channels. Although, one radio can have multiple channels, a single channel is used in each radio for simplicity of design and application.

Solution

It is assumed that the core network has achieved a stable connectivity state. This is a fair assumption as all wireless mesh gateways (WMGs) are installed by the provider and are not likely to be moved. The node initialization stage is for wireless mesh routers (WMRs) that are joining the network. WMRs can either be installed by the provider or a subscriber. The WMR performs a hardware check to ensure that all its hardware is functioning properly. It then starts sending out maintenance beacons (broadcast) every second at the base power level. Transmitting at the base power level helps ensure that the broadcasts do not impact the network unnecessarily. They also help assure that any nodes that receive it are definitely within good transmission range of the WMR. These beacons contain the following information:

- Enterprise Service Set ID (ESSID)

- Wireless Channels (WCH). This indicates what channels have been assigned to the network. It is set to zero (or unused) in a non-regulated environment.

- Cipher of ESSID and Subscriber/Node ID encrypted with the Service Provider's Private key.

- Node Status (NSTAT) – Bridge (B), Gateway (G), Subscriber (S), Access (A), None (Unused)

- One-way hash of Node Status (Bridge, Gateway, Subscriber, Access, None) and Subscriber/Node ID. WMGs have Node IDs(NID) instead of SID

These beacons are forwarded all over the network till they arrive at a WMG which forwards them to the core provider network. The core provider network contains the services that the network provides (authentication, authorization, accounting, billing, certificate services etc.)

Every WMR/WMG that receives this beacon sends a beacon back to the originating node (unicast). The node trying to initialize keeps track of the beacons it receives. If it receives a beacon from another node three times in succession (within a specified time period), it stores the transmitting node in its neighborhood table. If it receives a beacon from a WMG (as indicated by the node status) and verifies it by decrypting the cipher of the ESSID and NID, it stores it immediately.

In the event that the node receives multiple beacons that satisfy the requirements above e.g. when there is dense connectivity, the WMR does the following to select the nodes to put in its neighborhood table:

The three nodes with the highest RSSI are put in the neighborhood table. These three nodes could be WMGs (which indicates that the node is closer to the 'top' of the network) or WMRs (which indicates that the node is closer to the 'bottom' of the network) or a mixture of both.

WMGs are always preferred over WMRs.

• Other nodes with RSSIs above a certain threshold are put in an alternate neighborhood table. If two nodes have the same RSSI, the node with the newer SID or NID is put in the neighborhood table while the other is put in the alternate neighborhood table. In the unlikely event that two nodes have the same SID or NID, the node selects whichever beacon was received first.

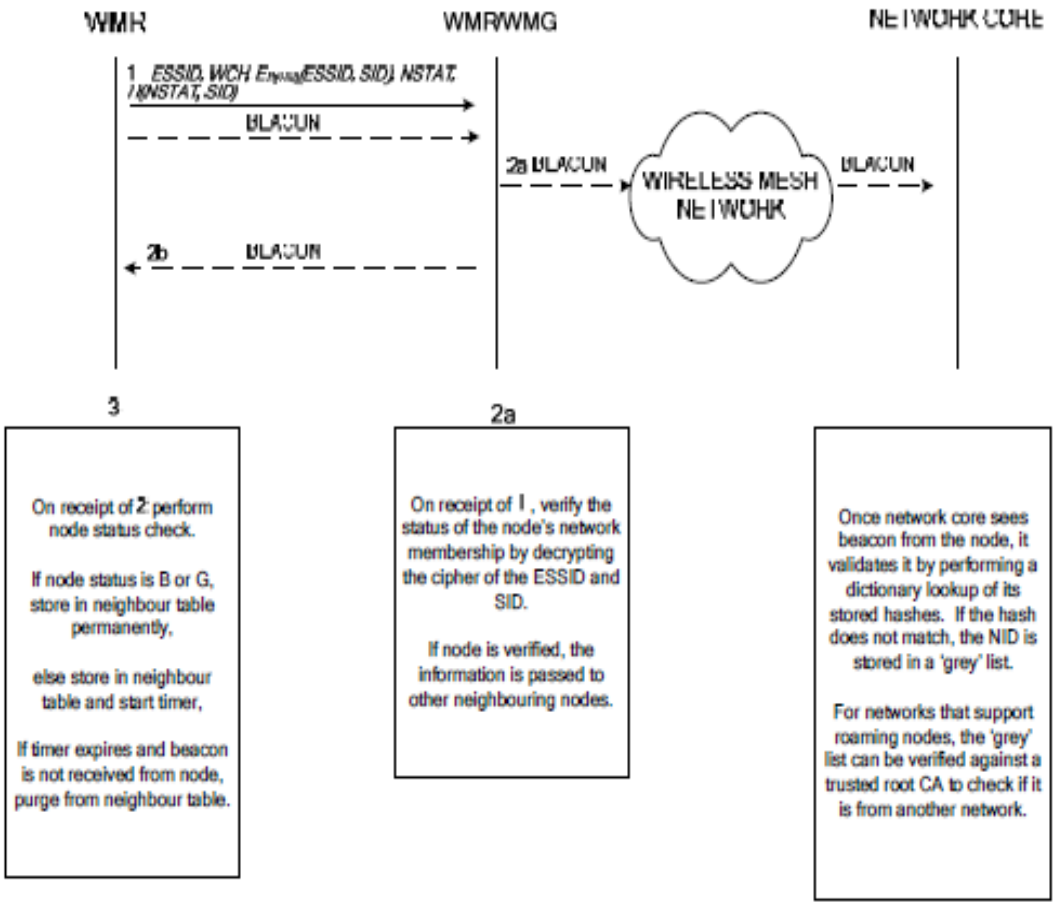
The alternate neighbor table serves two main purposes:

It is used for rapid rebuilding of a node's neighborhood in case one of its preferred neighbors fails.

2. It can help alleviate contention for resources. This can help achieve load sharing in the network by diverting traffic away from overloaded nodes.

At the end of this stage, the WMR should have its neighborhood list complete

Protocol Flow Diagram – Node Initialization



NODE BOOTSTRAPPING

After the node initializes, it has to properly join the network topology. This is especially important in wireless networks as the ability to sense a node does not necessarily mean it is best to communicate using that node. This stage is known as node bootstrapping. The node uses the information gained from the initialization stage (neighborhood list, RF properties etc.) for this stage. This ensures that the phase can be completed as quickly as possible.

Solution

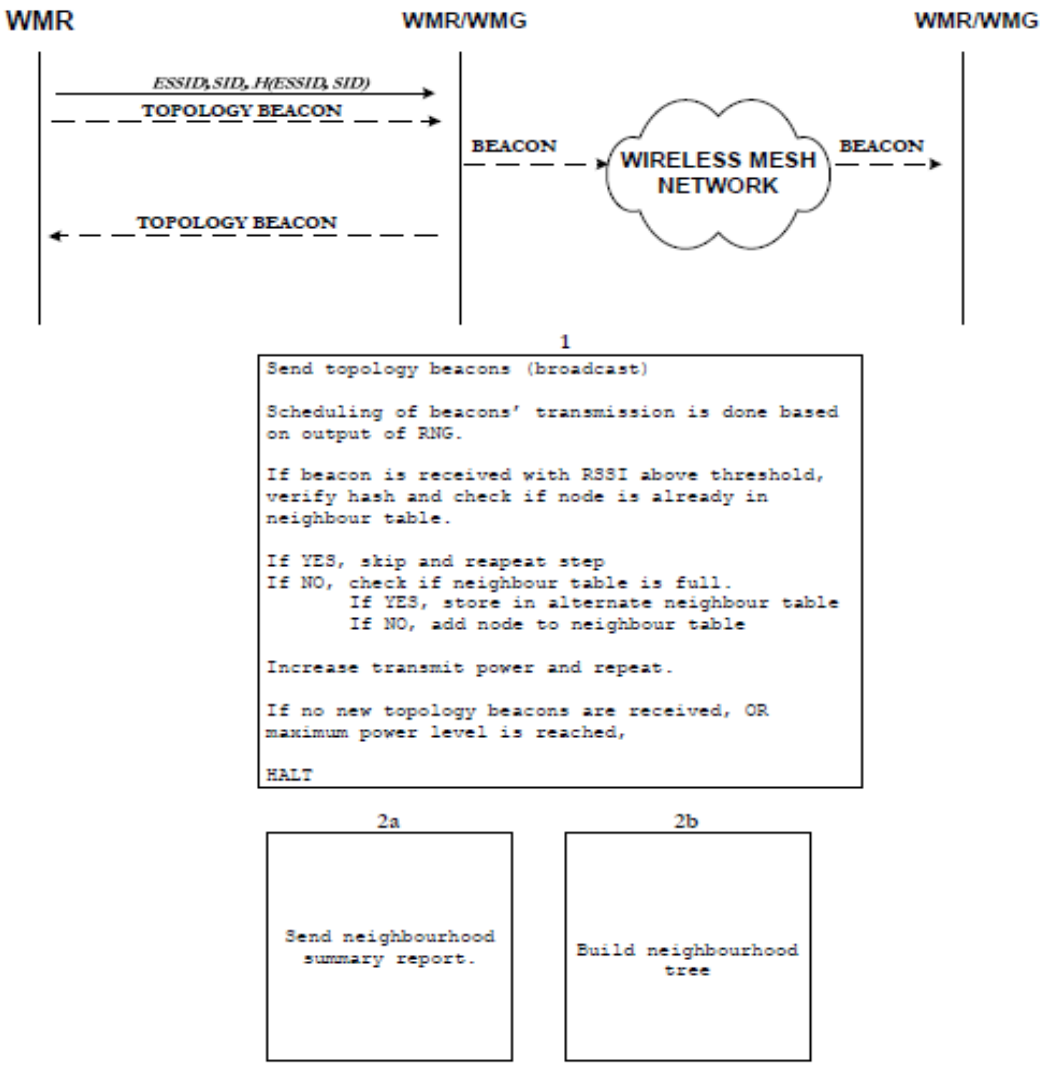
As nodes receive and send beacons, the node gathers information about the topology network. The node is able to establish its neighborhood and determine which nodes it can ‘hear’ clearly. This achieves two objectives: a. If all checks pass, it means the node is a valid member of the network and can be reasonably determined to be under the control of a valid subscriber. If this is a guest node from a foreign network, the node still gets connected from a topology perspective but is not allowed to utilize any network services until the Network registration stage (described below) is complete. Also, no local nodes will be able to pass any application traffic until after the Network registration phase.

Nodes that sense multiple "collision neighborhoods" are designated "sponsor nodes" or "bridge nodes" (i.e. summary reports from multiple nodes contain different node sets). The Gateway nodes are predetermined by the service provider as they are the nodes that constitute the wireless backhaul. The closest neighbors will be determined based on received signal strength (RSS) and they will agree on a common channel based on the wireless technology used for the network. The complexity of this stage is that wireless links are not necessarily bidirectional and orthogonal channels (especially in 802.11 b/g) are scarce. The likelihood that a node will be in multiple collision neighborhoods is high (especially in dense WMNs).

Each node sends out a summary report (broadcast) with all the nodes in its collision neighborhood to other nodes after the bootstrapping stage is complete. Based

of all the received reports, each node builds a subtree with itself as the root (combined with the RSS information from the topology beacons) with paths chosen optimally. This is a reactionary process. Only nodes who lose paths will broadcast a new summary report which may or may not trigger path calculations at other nodes

Process Flow Diagram – Node Bootstrapping



CAPACITY MODELS

The capacity of a multi-hop wireless network is the traffic payload that it can transport. This is a prominent quality of service issue, particularly in the highly constrained settings of 802.11 wireless mesh network. A network-wise capacity is defined as the sum of the upload traffic, and a flow-wise capacity highlighting the unfairness among traffic flows.

Two complementary definitions of the capacity

A first one, denoted network-wise capacity, is a measurement of the behavior of the whole network. It is defined as the sum of the traffics that have reached the gateways to the Internet.

A second one, denoted flow-wise capacity, measures the capacity of each flow, that is the quantity of bandwidth allocated to the traffic collected by each router. To combine these two notions of capacity allows to highlight the unfairness among flows in network, which is a user-oriented point-of-view, within an operator-oriented look at the average behavior of the infrastructure.

Routing protocols

Consider four routing protocols in order to route the upload traffic from the routers to the gateways.

Shortest path routing

This routing protocol is based on the Dijkstra algorithm. The goal is to find the shortest path in terms of hops between source and destination. The global knowledge of the whole topology is necessary and obtained using periodic control packets.

Geographic routing protocol

This routing protocol is based on the knowledge of geographic position for each node using GPS-like positioning. The main idea is to compare, at each hop, the euclidean distance between all neighbors and the destination, and choose to forward the packet to the closest neighbor.

Random routing protocol

This routing is based on a random walk. It means that at each hop, the packet is forwarded to a randomly chosen neighbor. This protocol does not require the knowledge of the whole network, but only the neighborhood of each router using hello packets.

Two strategies are used to improve the behavior of this protocol:

i) the packet is sent to the destination if it is a neighbor and

ii) ii) a packet is never routed to a node which has no other neighbor.

Static routing protocol

With this routing protocol, all the paths between source node and destination are manually entered. This protocol does not require the use of control packets.

Performance evaluation criteria

Network capacity

In our work, the network-wise capacity is the quantity of traffic sent by all nodes (N) and forwarded to the Internet through the gateways (K) during the simulation period. It is a view of the global bandwidth of the network shared among all nodes.

This metric represents the maximum quantity of traffic that the network can transmit to the Internet. A better network-wise capacity is necessary for providing a better quality of service to a larger number of users.

This metric is calculated as follows.

$$C_{\text{network}} = \frac{\sum_{k \in \mathbb{K}} \sum_{n \in \mathbb{N}} |\text{Received\_packets}(n \rightarrow \text{k})|}{\text{Simulation\_time}}$$

This metric does not illustrate the unfairness problem in the network. A more detailed view is necessary for taking into account the bandwidth allocated to each flow.

Flow capacity

It is defined by the sum of traffics sent by a router and received by the gateway during the observation period. This metric illustrates the bandwidth consumed by each router in the network. Thus, it allows to study the problem of unfairness in the distribution of bandwidth amonog the flows. This is a key point of the quality of service. In fact, an operator must ensure a bandwidth acceptable for each node in the network.

This metric is calculated as follows.

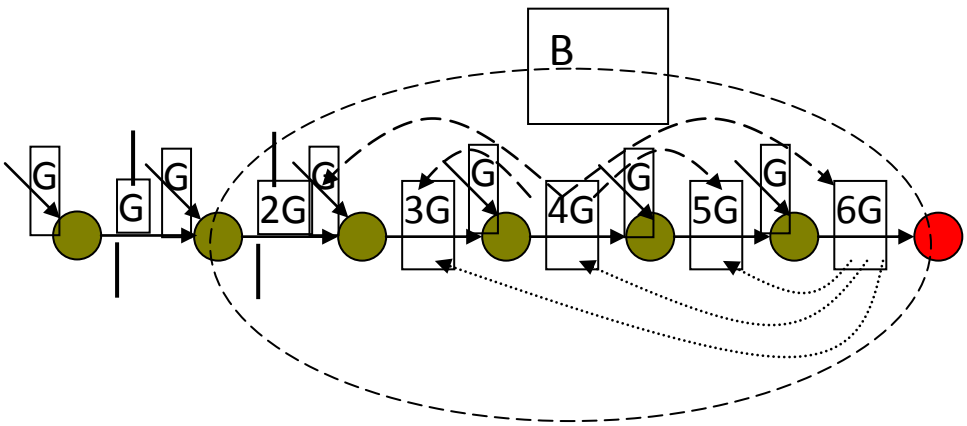
$$C_{\text{flow(n)}} = \frac{\sum_{k \in \mathbb{K}} |\text{Received\_packets}(n \rightarrow k)|}{\text{Simulation\_time}}$$

These two metrics are complementary because the first gives a global vision of the network while the second gives a detailed view.

Two capacity models:

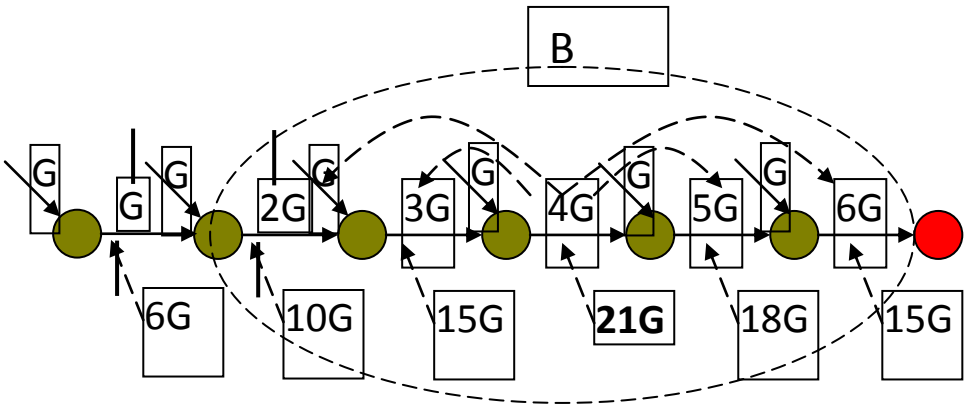
- Clique is more-accurate (single channel)
    - But requires information that may not generally be available
- Collision domain approach is very close to accurate
    - Within the deviation of the two models
    - Computed with readily available information
- Neither model is accurate in the presence of RTS/CTS

Example: Clique Model



Gmax = B/18

Example: CD Model

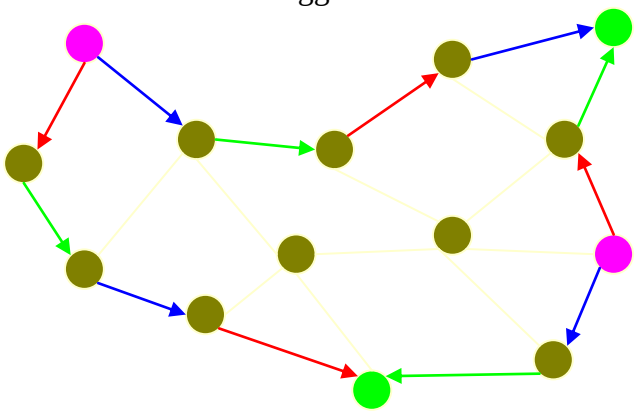


Gmax = B/21

- Compare to calculated capacity
  - Clique model under-estimates by 0.07%, on average
  - Collision domain model under-estimates by 2.3% on average
  - Deviation in ~10% in both cases

Capacity Problems

- Efficient use suggests multi-channel routing



Approaches

- **Multi-channel, one radio**
  - Cheaper
  - Switching delay
  - Same (or worse) delay as single-channel in a given hop
    - In, then out separately
  - But better over multiple hops
- **Multi-channel, multi-radio**
  - More radios: more expensive
  - But still relatively cheap
  - But they interfere with each other
    - Use one in 2.4 GHz and one in 5 GHz band
- **Access vs. backhaul separation**
  - *e.g.* Nortel approach
- **Multi-radio backhaul**

Multi-radio capacity

- Generalize capacity models by creating N sub-graphs, one per channel, and then using the same basic approach on each sub-graph
- Clique performs poorly in three-channel, two interface case
- Collision Domain is largely accurate

HETEROGENEOUS MESH NETWORK

Heterogeneous mesh network is the combination of different types of mesh networks to improve the performance of the network. The major obstacles of large Wi-Fi mesh network include low capacity, limited system performance, and the uncertainty of mesh topologies and wireless link quality.

Possible reasons for those problems inside large mesh networks are listed as follows.

1. First, multihop transmission is one of the major reasons that limit the system performance. Since not all mesh nodes have direct connection to their final destinations, multihop transmissions are inevitable. However, the performance of multihop transmission decreases quickly as the number of hops increases. Packets that traverse through more hops either have little opportunity to reach the destination, or consume too much network resource, both of which decrease the system capacity and increase delay and congestion.
2. Second, to take advantage of existing APs to construct a wide-area mesh network, the network topology is not always under control. Due to network topology and link or node failures, some mesh nodes (known as island nodes) may fail to find available paths to the portals. Depending on specific topologies and failure probabilities, the proportion of island nodes may not be negligible.
3. Third, in large mesh networks, centralized MAClayer schemes, global link transmission scheduling, or synchronization are not practical. Therefore, hidden terminals [23, 24] could cause collisions and further reduce the capacity.
4. Fourth, because of the traffic dynamics, Wi-Fi mesh network is prone to network congestions and congested links negatively influence the performance of mesh networks.

Motivation for Hybrid Wi-Fi/WiMAX Networks

WiMAX was originally designed for point-to-point broadband wireless transmission over long distance, and operated at 5 GHz, which requires line-of-sight transmission. Recently, with the quick development of WiMAX technology and additional spectrum availability (2.3, 2.5, 3.5, 3.7 and 5 GHz), it can support both outdoor and indoor, as well as both fixed and mobile scenarios.

However, large-scale wide-area meshes may not be efficient and cost-effective if we use only WiMAX.

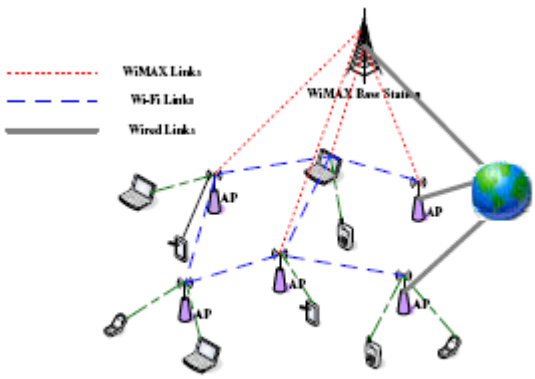
1. First and most importantly, although the large coverage of WiMAX reduces the number of wireless hops in the network, it cannot support good spatial-reuse of spectrum; while Wi-Fi has been proven to be a good solution.
2. Second, WiMAX devices have much higher power consumption and are much more expensive than Wi-Fi devices.
3. Third, from the economical aspect, Wi- Fi devices have been widely deployed, and therefore it is beneficial to integrate WiMAX networks with existing Wi-Fi networks.

Advantages

- The deep penetration of Wi-Fi networks provides good throughput and large (but not ubiquitous) coverage at low cost.
- On the other hand, the long range transmission of WiMAX can effectively solve the major problems in large Wi-Fi mesh networks.
- First, the presence of WiMAX networks alleviates the need to transmit over a large number of hops.
- Far-away nodes can forward traffic through WiMAX networks, while traffic generated by the nodes near portals still go through Wi-Fi.

- A good proportion of multihop wireless transmissions are replaced by one-hop wireless transmission through WiMAX.
- In addition, the hidden terminals would also become less severe with shorter paths. Second, island nodes with dual interfaces can connect to WiMAX, and thus network coverage is improved.
- In addition, WiMAX can provide reliable transmission in a large area. And thus, the heterogeneous network is robust and can provide ubiquitous wireless access in the presence of link/node failures.
- Third, the existence of WiMAX with large coverage area enables statistical multiplexing, which effectively reduces network congestion due to traffic dynamics and topology limitation of WiFi-Only mesh networks.
- Another characteristic of WiMAX and Wi-Fi networks is that they can coexist without interference as long as they operate on different spectrums.

Architecture



There are **three kinds of nodes**,

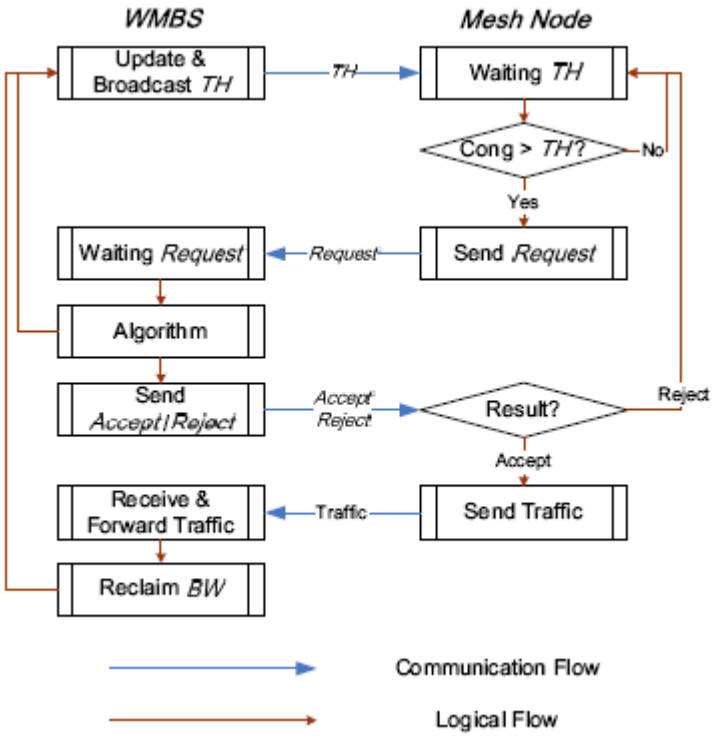
- customer terminals such as laptops, PDAs and smart cell phones,
- mesh nodes such as APs and laptops with routing function, and
- WiMAX base stations (WMBS).

These nodes cooperate to forward traffic from the individual customers to the Internet or peers inside the mesh network. Customer terminals have only Wi-Fi interfaces and send packets to the nearby mesh nodes; mesh nodes could either have only Wi-Fi devices and relay packets through multihop Wi-Fi mesh networks or have both Wi-Fi interfaces and WiMAX subscriber interfaces, and relay packets through two networks; WMBSs only have WiMAX interfaces, and can communicate with mesh nodes with WiMAX interfaces.

Therefore there are **three kinds of wireless connections**, customer terminals-mesh nodes, mesh nodes-mesh nodes, and mesh nodes-WMBSs. For coexistence of the first two kinds of connections that share Wi-Fi interfaces, some solutions have been proposed, such as multiple-radio and multiplechannel, and partially overlapped channel transmission.

Besides the wireless connections, wired links in the system provide reliable connection to the Internet with high capacity. As shown in Figure, portals and WMBS are nodes with wired connections. They are usually traffic aggregation points if the destinations of packets are remote servers in the Internet. Note that first only some of mesh nodes are portals; second some portals may have both Wi-Fi/WiMAX devices, which helps when the packet destinations are other mesh nodes in the network.

PROTOCOL AND ALGORITHM DESIGN



It is necessary to design a protocol that can achieve the gain in practice and deal with challenges that are not captured by the idealized model. In a practical system, the protocol needs to allocate resources based on the information of the dynamic network conditions, such as link capacity and traffic demand. Unfortunately, accurate realtime information is hard to obtain, so the protocols need to perform under network information with delay and inaccuracy. In addition, complicated protocols with high overhead are not suitable for wireless networks since the wireless transmission resource, time or bandwidth, is very precious. The threshold-based protocol and an optimization algorithm, which answer two basic questions: (1) which mesh nodes

connect to the WiMAX network, and (2) the amount of traffic mesh nodes forward to the WiMAX network.

Assumptions and Objective

1) WiMAX utilizes the scheduled MAC scheme.

2) In Wi-Fi networks, nodes utilize IEEE 802.11 MAC instead of the scheduled MAC as in theoretical study.

3) The WMBSs do not try to control the routing or scheduling inside the Wi-Fi network.

The last assumption preserves the basic properties of Wi-Fi mesh networks: the easy extension and independent routing. The objective is to minimize the maximum utilization inside the whole network. Since it is too complicated to synchronize link scheduling in practical networks, our only decision variable is the routing variable, which determines the amount of traffic going through the Wi-Fi or WiMAX networks.

VEHICULAR MESH NETWORK

Vehicular communication has mainly focused on supporting two broad categories of applications:

a) **vehicular safety**, such as exchanging safety relevant information or remote diagnostics using data from sensors built into vehicles

b) **mobile internet access**. However, there is a large untapped potential of using such vehicular networks as powerful and distributed computing platforms or as transit networks.

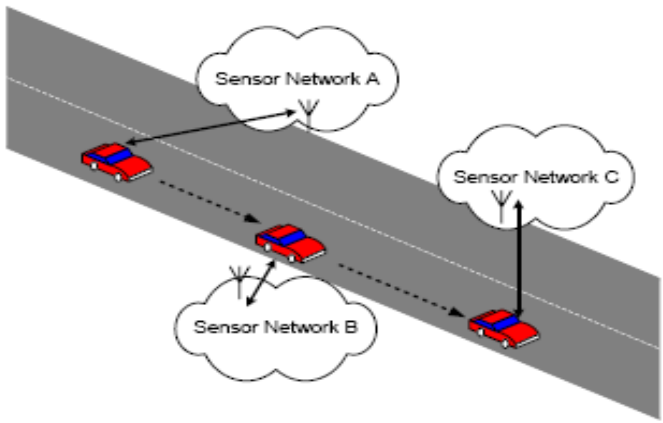
Vehicular networks have very **different properties and design challenges** compared to their counterparts such as laptops in nomad computing or sensor networks.

- First, vehicles travel at a much higher speed, making it challenging to sustain communications between stationary sites and moving vehicles, as well as handing-off the communication link from one site to the other as the vehicles pass between them.
- Second, despite the common assumption of random mobility patterns in many simulation studies on ad hoc networks, the vehicular traffic has a more well defined structure that depends on the transportation grid (highway, city roads, etc).
- Lastly, vehicles, as communication nodes, have abundant life and computing power as compared to sensor networks.

A mesh network is an ad-hoc network with no centralized authority or infrastructure. Nodes can move, be added or deleted, and the network will realign itself.

The benefits of a mesh network are that it has the abilities of self-forming, self-healing, and self-balancing. As shown in Figure, one of the applications of using VMesh as a transit network is to establish connections between disjoint sensor networks.

Using VMesh to connect disjoint sensor networks



VMesh can be used to interconnect the sensors and the backbone wide area network (WAN) infrastructure, e.g., Internet backbone, wireless cellular infrastructure, DSL or Cable. These vehicles, or MRs, are responsible for disseminating price information to and retrieving information from different households to support dynamic tariffs and demand-response.

In this case, VMesh is designed to meet the following **goals**:

• **Low Deployment and Maintenance Cost:** Since the routers in this case are ”mobile”, one can drive these mobile routers into a station (e.g., main bus station or police headquarters) for repairs or software/hardware upgrades, instead of having to send a repair team out to various locations to fix the problems if they were stationary. Moreover, the number of mobile routers required can be minimized, e.g., using buses traveling on different routes is sufficient to cover the entire city. Hence, both the installation and maintenance costs are greatly reduced.

• **Adaptive Fidelity:** By using a combination of vehicles as mobile routers, VMesh provides a wide spectrum of flexibility in terms of the frequency of message retrieving and the granularity of demand response control loops. For example, while buses run

every 0.5 - 1 hour, they do not stop at every single household. On the other hand, garbage trucks may stop at every household but they only come by once a week.

• **Scalability:** VMesh can support incremental deployment easily as the number of sensor nodes grows. In fact, VMesh benefits from the economy of scales, i.e., the cost of introducing a new mobile router goes down as the number of sensor nodes it is capable of serving increases.

• **Broadcast and Multicast Capabilities:** Broadcast and multicast capabilities are inherent in the wireless communications used between the mobile routers and sensor nodes, between the mobile routers and aggregation points to the VMesh network backbone, and between mobile routers and other vehicles equipped with wireless transceivers.

• **High Level of Redundancy:** VMesh has a high level of built-in redundancy by leveraging different vehicles that overlap in spatial coverage and temporal samplings. For

example, there may be different routes for public transit through the city, but these routes often overlap in the main streets. In addition, garbage and postal trucks will visit the households on the same street at different times of the day. Therefore, the same end-user can be connected by two or three different types of vehicles. There are multiple available paths to ensure the delivery of the DR messages.

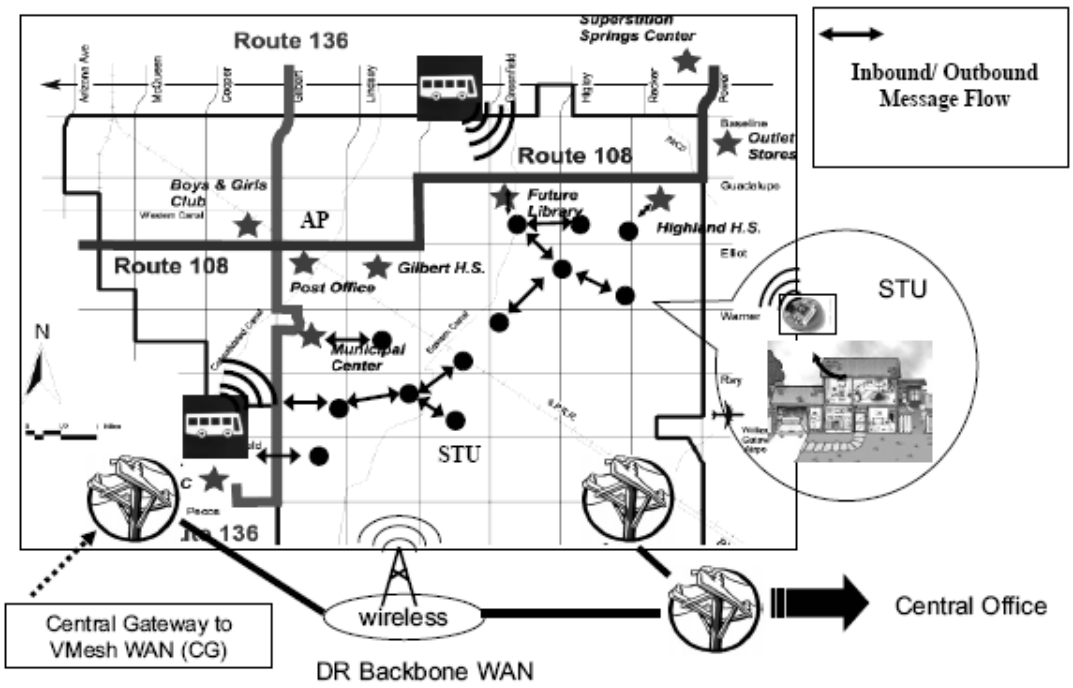
• **Failure Resiliency via Deflection Routing:** VMesh ensures the survivability of the DR messages by deploying the deflection routing technique. The key premise lies in the ability of VMesh to deflect messages until a valid path is found to the destination instead of dropping them when the original path fails due to faulty mobile routers, broken communication links, or vehicular accidents. DR is one type of applications the VMesh network is capable of supporting. In addition to supporting demand response,

VMesh also enables the deployment of other large-scale societal applications such as amber alert (e.g., broadcasting information of a kidnapper's vehicle and detecting this moving target), vehicular traffic control, and temperature/air-pollution monitoring. In the next section, we will first introduce a generic VMesh network architecture and then describe the method to support DR with this generic architecture.

VMESH ARCHITECTURE

Vehicular mesh networks are ad hoc networks formed by vehicles enabled with wireless networking. As the vehicles move, the connectivity between the vehicles and other static network nodes changes. The network is dynamic and as a result, nodes may be disconnected from the network at times. To address this, nodes will store the data during the period they are disconnected from the network.

An **example vehicular mesh network** is shown in Figure.



The figure shows two bus routes (Route 136 and Route 108) and some key components of VMesh. The key components of the architecture are as follows:

1) **Sensing and Transceiving Units (STUs)** are wireless enabled sensors that will transmit collected data to the central office (inbound message). They also receive new

configurations such as new pricing information generated by the central office (outbound message). These are shown as solid circles in Figure. If STUs cannot directly connect to the VMesh backbone network, they can form a network themselves to route inbound and outbound messages.

2) **Aggregation Points (APs)** are nodes that act as gateways to the VMesh. They can aggregate inbound messages, relay the messages to the VMesh, accept outbound messages, and route these outbound messages to one or more STUs. These gateways could be special nodes deployed at appropriate locations or specific STUs that are enabled with the gateway functionality.

3) **Mobile Routers (MRs)** are wireless enabled mobile objects that have the ability to store and forward data. For example, buses, along with other various types of vehicles equipped with storage and wireless networking, form ad hoc networks with other mobile routers and connect to the static gateways.

4) **Central Gateways to VMesh (CGs)** are gateways which connect different VMesh networks. These are located at specific locations on the paths of mobile routers, such as at the main terminal stop of buses. The characteristics of VMesh depend on the mobility pattern of the participating mobile routers as well as neighboring vehicles. The choice of vehicles that are suitable for VMesh heavily depends on their attributes which include:

1) **Coverage**: How many STUs are directly accessed? We refer to the coverage as being fine-grain if the MRs can directly access individual or small groups of STUs directly.

2) **Schedule and Periodicity**: Is there a fixed schedule in the mobility pattern of MRs and if so, what is the period?

3) **Redundancy**: Are STUs or APs covered by multiple MRs? Are there multiple paths from the individual STUs to the APs?

4) **Cost**: What is the cost of deployment and maintenance in terms of the number of STUs, MRs, and APs?

For example, buses provide coverage to almost every major street in a dense major city such as San Francisco and their schedules coincide with peak electricity usage (e.g., buses run more frequently during work hours when energy consumption is high than at night). The mobility pattern of the vehicles depends on the type of vehicles, which include personal automobiles, public transport buses and light rails, postal vans, garbage trucks, various types of vendor trucks and vans such as UPS and FedEx, law enforcement vehicles such as police cars, and other monitoring vehicles such as those that monitor parking violations.

Various types of MRs for a VMesh in suburban area

	cars	Buses	Postal Vans	Garbage Trucks	Vendor Trucks	Police Cars
Coverage	Fine (1-10 m)	Coarse (10-1000 m)	Fine (1-10 m)	Fine (1-10 m)	Coarse (10-1000 m)	Coarse (10-1000 m)
Schedule	Regular	Regular	Regular	Regular	Random	Random
Period	24 hrs	15 mins	12/24 hrs	7 days	Few Hours	None
Redundancy	Low	Medium	Low	Low	Medium	High
Cost	High	Low	Low	Low	Low	Low

Various types of vehicular mesh networks can be characterized along these parameters depending on the targeted geographic area. An example of such characterization for a suburban area is shown in Table. For the case of demand response, DR is enabled in

the following manner. Periodically, the sensors transmit collected data that are routed to one or more aggregation points through a local ad-hoc network. When the mobile router travels by these aggregation points, it downloads the collected data and uploads new configurations which are distributed to the sensor nodes using local ad-hoc networks as well. The collected data can be opportunistically routed by the vehicular mesh network to the central gateways. In the worst case, the central gateway may be located at the terminal point of the route of the mobile router

ROUTING IN VMESH

The Greedy Perimeter Stateless Routing (GPSR) as the backbone algorithm to send data from sensors to APs. In GPSR, need to establish a planar network, such as a Gabriel Graph (GG) or Related Neighborhood Graph (RNG) to eliminate intersecting edges in the network. After that, two routing algorithms, greedy forwarding and perimeter routing, are used to deliver packets. GPSR uses the *most forwards within radius* (MFR) greedy algorithm as the general packet forwarding algorithm to minimize hop counts.