INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL and MECHATRONICS ENGINEERING
Vol.2 Num.1 pp.(92-104)

A SURVEY on WIRELESS MESH NETWORKS, ROUTING METRICS and PROTOCOLS

Safak DURUKAN ODABASI[1], A. Halim ZAIM[2]

[1] Department of Computer Engineering, Istanbul University, 34320, Avcilar, Istanbul, Turkey
***E-mail:** sdurukan@istanbul.edu.tr*

[2] Department of Computer Engineering, Istanbul Commerce University, 34840, Kucukyali, Istanbul, Turkey
***E-mail:** azaim@iticu.edu.tr*

Abstract: *Today, Internet has become an indispensable part of our daily lives. It has a growing user community in many fields from banking transactions to online entertainment. It will be very efficient for users, as the next generation internet access becomes wireless like frequently used services such as cellular phones. But for providing this, a new network is needed to be designed or an existing network must be improved as well as making changes on infrastructure. At this point, mesh network infrastructure arises and offers more sophisticated internet access with less need. The most important advantage of mesh networks is the capability of working without infrastructure. Mesh networks are an additional access technology more than being a renewed one in the next generation wireless networks called 4G.*

In this study, wireless mesh networks and example applications are mentioned. Base architecture and design factors are emphasized, current routing protocols that are used on wireless mesh networks and routing metrics on which these protocols are based, are explained. Finally, the performance effects of these protocols and metrics on different network topologies are referred.

Keywords: Wireless Mesh Networks (WMN), routing metrics, protocols

I. INTRODUCTION

There is no doubt that, wireless communication has been a desired service with the rapid improvement in cellular and wireless local area networks. These two different technologies come close in the terms of their needs and with this cooperation, numerous applications have become available.

There are currently two variations of mobile wireless networks [1]. The first is known as the "infrastructured network". It is a network which has fixed and wired gateways. The bridges for these networks are known as "base stations". Typical applications of this type of networks include office wireless local area networks (WLANs).

The second type is infrastructureless and these types of networks are known as "self-organized networks". They consist of mobile radio nodes which do not need existing network infrastructure or central system management. They are suitable for situations that need an immediate infrastructure.

Next generation services will provide high data rates, overall flexibility on sending and receiving levels, lower equipment cost and capacity of arriving to all subscribers. At that point, to solve all of these problems, a new concept called Wireless Mesh Network (WMN) has been proposed. WMN is a new technology area that will take a hand in next generation wireless mobile networks.

II. WIRELESS MESH NETWORKS – WMNS

In contrast to traditional wireless networks, WMNs are not built on a fixed infrastructure. Instead of this, hosts rely on each other to keep the connection. WMNs provide low-cost broadband internet access, wireless LAN coverage and network connection to fixed or mobile hosts for both network operators and users. The reason of preferring WMNs is easy, fast and deployment of the technology.

A typical WMN consists of mesh routers and mesh clients [2]. Mesh routers are fixed. They have a wireless infrastructure and work with the other networks to provide a multi-hop internet access service for mesh clients. On the other hand, mesh clients can connect to network over both mesh routers and other clients. In these networks, due to large number of nodes, working through some issues like security, scalability and manageability is required. Thus, new applications of WMNs make secrecy and security mechanisms are necessities.

The main problem of this technology is the complexity of WMNs. Although design, deployment and transmission of packets are easy, it is really hard to reach an optimum performance to provide security and robustness.

III. ARCHITECTURE OF WIRELESS MESH NETWORKS

WMN routers need to have extra operation capacity to support mesh routing besides normal router duties. Thus, they have more than one network interface card (NIC). Mesh clients usually have one NIC. Because they do not require having some features like bridge and gateway. WMNs can be classified in three types [3]:

- **Infrastructure / Backbone WMNs:** Infrastructure WMN architecture is shown in Figure 1 [3]. This kind of WMNs has dozens of interconnecting clients. Connection between routers, internet and other clients is set by cables (as shown with straight lines) or wireless links (as shown with dashed lines). WMN backbone mainly uses IEEE 802.11 technology within various wireless technologies.

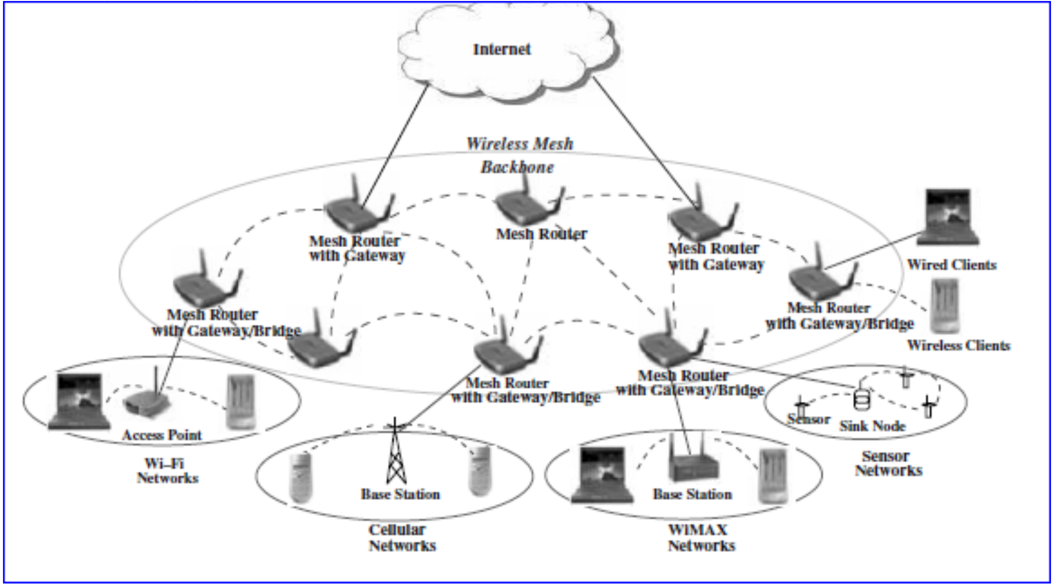


Fig. 1: Infrastructure/backbone WMN.

- **Client WMNs:** A router is not necessary on the networks which are established between clients as P2P. In this case, highest level of data transmission occurs. A packet is sent to reach a destination through multinodes. All traffic crosses over single nodes in the network. In this kind of WMNs, nodes require to have routing and self-organization functionalities.

- **Hybrid WMNs:** An additional network structure covers the existing mesh network and controls long-distance packet traffic. A hybrid WMN has infrastructure and client WMNs as shown in Figure 2 [3]. While the infrastructure part provides the connection between mesh and the internet, Wi-Fi and WiMAX networks; clients' part organizes routing processes.

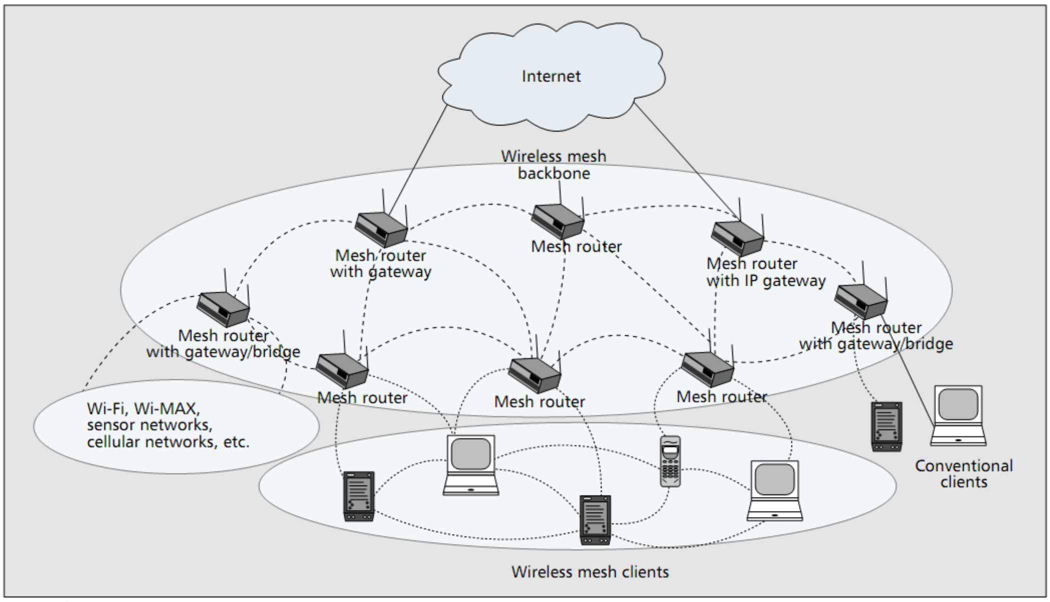


Fig. 2: Hybrid WMN.

III.I. The Characteristic Properties of Wireless Mesh Networks

Main characteristic properties of WMNs can be outlined as seen below:

- To solve Line-of-Sight (LoS) problem especially on central wireless networks, WMNs send packets over multiple nodes, so packet loss rate can be minimized.
- Addition or subtraction to network can be made easily after network deployment. Network can be enlarged or narrowed. Coverage and interactivity are uncontrolled.
- WMNs have the functionality of P2P network as well as accessibility to different network environments and technologies smoothly.
- WMNs do not have energy consumption constraints unlike existing protocols. Energy efficiency is not placed on the top in terms of priority on WMNs.
- They conform with current wireless network technologies. As WMNs use IEEE 802.11 technology, other communicated networks should predicate this technology on.
- Ensuring and carriage of functionality are provided with mesh. Accomplishment of these issues includes routing, security, management and power control.
- Nodes are free on their movement. They can change their networks and move between cells. Thus, WMNs have a very dynamic structure.
- Wireless operation is necessary for supporting mobility. So, signals and optical hardware can be used to provide wireless operation.
- All nodes must join a routing process on the network.

Therefore, WMNs diversify the capabilities of ad-hoc networks instead of simply being another type of ad hoc network. These additional capabilities necessitate new algorithms and design principles for the realization of WMNs [3;4] .

III.II. Design Factors of Mesh Technologies

The internet technology is made up of logically organized layers. Each layer has some definite features to transmit data and communicate properly [4;5;6]. If we think these layers as a generic communications protocol stack, the layers can be shown as in Figure 3 [4].

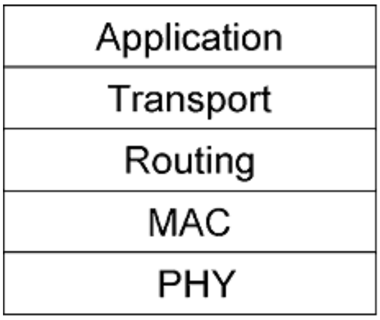


Fig. 3: Layers of a network.

Physical layer (PHY) is the bottom layer and has an air-interface that is concerned with antennas and radio electronic systems directly. But there is not any information about how this equipment reaches to this air-interface on the PHY layer. Medium Access Control (MAC) layer is responsible for this task. In MAC layer, there are plans for sharing this internet medium by multiple users.

A kind of addressing mechanism is needed to find necessary nodes and communicate with other nodes. Routing layer handles this task.

Next layer is transport layer. It is the responsible layer for delivering packets to their destinations. The most known and used transmission protocol in this layer is TCP.

Application layer is the last layer that offers an interface to users.

There are some critical performance factors for WMNs on network design and application.

- **Signal Transmission Techniques:** Many approaches have been proposed to increase capacity and flexibility of wireless systems in recent years [1]. In conjunction with the development of marketplace techniques, there has been a great evolution in the wireless communication area. To further improve the performance of a wireless radio and control by higher layer protocols, more advanced radio technologies have been used for wireless communication. Although these radio technologies are still in their infancy, they are expected to be the future platform for wireless networks due to their dynamic control capability. These advanced wireless radio technologies all require a revolutionary design in higher-layer protocols, especially MAC and routing protocols and signal transmission techniques should proceed to attack as soon as new products are put out.
- **Scalability:** In multihop networks, communication protocols encounter a problem of scalability. As long as the network size grows, system performance decreases substantially. The main reason of this problem is falling of end-to-end reliability by decreasing of performance. In order to increase scalability, a hybrid structure of TDMA, CDMA and CSMA-CA should be used.
- **Mesh Connectivity:** WMNs have the advantages of mesh connectivity. Network self-organization and topology control algorithms should be used to provide reliable mesh connectivity. Topology-aware MAC and routing protocols can significantly improve the performance of WMNs.
- **Broadband and QoS:** WMNs need heterogeneous QoS supports unlike traditional ad-hoc networks. Thus, in addition to end-to-end transmission delay and fairness, additional performance metrics, such as delay jitter, aggregate and per-node throughput, and packet loss ratios, must be considered by communication protocols.
- **Security:** There are so many security mechanisms for WLANs but none of them is suitable for WMNs. Because WMNs have a distributed system architecture. The existing security schemes proposed for ad hoc networks can be adopted for WMNs.
- **Ease of Use:** Protocols must be designed to enable the network to be as autonomous as possible. In addition, network management tools need to be developed to efficiently maintain the operation, monitor the performance, and configure the parameters of WMNs. These tools, together with the autonomous mechanisms in networking protocols, enable rapid deployment of WMNs.
- **Compatibility and Inter-operability:** In WMNs, it is a default requirement to support network access for both conventional and mesh clients. Therefore, WMNs need to be backward compatible with conventional client nodes. This demands that mesh routers need to be capable of integrating heterogeneous wireless networks.

III.III. Wireless Mesh Network Applications

WMNs can meet the needs of multiple applications

[6]. Wireless network applications have many dead points as they stand. Coverage of broadband home network which is set by WMN can be decreased without using additional physical hardware. To improve the coverage, changing the positions of mesh routers or just adjusting the signal power is enough. Ad hoc and wireless sensor networks are not appropriate to support such applications. WMNs are ideal in this case due to their load balancing property.

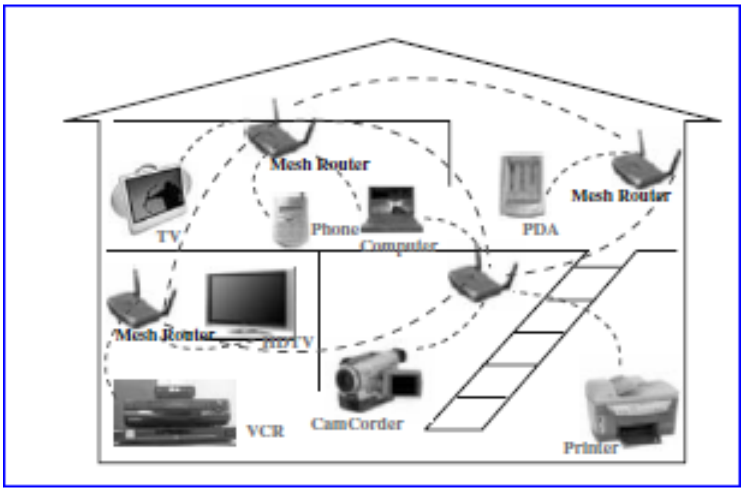


Fig. 4: Short-Distance Home Mesh Network.

As shown in Figure 4 [3], a home mesh network can easily be set up. In the same way, it is possible to connect more than one house, a street even a city by using a mesh router chain. Especially in the terms of cost, the cost of setting up a network with cable and existing IEEE 802.11 WLAN routers would be more and leaner than WMNs.

As shown in Figure 5 [3], a mesh network with comprehensive routers can be used everywhere in a city and propose an overall coverage.

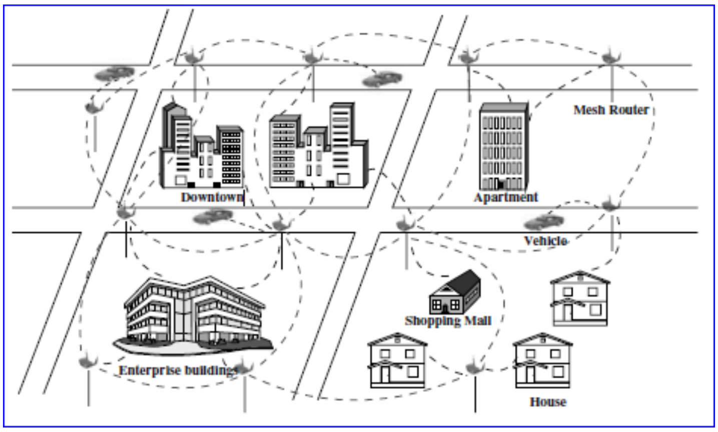


Fig. 5: Multihop Mesh Network in a City.

Various examples of WMN applications can be specified as below [7]:

- Cellular or WLAN hotspot multihopping
- Community networking
- Home and office indoor networking
- Micro base station backhaul
- Vehicular ad hoc networks (VANETs)
- Wireless sensor networks (WSNs)

III.IV. Challenges and Advantages of WMNs

The biggest advantage of mesh technology is the ability of working without dependence of any infrastructure. Some features like low-cost, easy network maintenance, robustness, and reliable service coverage allow WMN to stand out among existing technologies.

The primary advantages of WMNs are [7]:

- High coverage area even on low user density
- Excellent spectral efficiency and capacity
- No need of base station, therefore low

interference

- Complex flexibility on services
- Automatic antenna point
- Minimized configuration period.

On the other hand, there are some challenges which effect WMN design. Large number of nodes increases the complexity which also turns network into a target from the point of security, reliability and manageability.

IV. ROUTING ON WMNs

Routing protocols for self-organized networks are expected to provide some functions like detecting and responding to changes in network topology and services, providing management, constructing and selecting routes, maximizing the capacity of the network and minimizing the packet delivery delays [8].

IV.I. Routing Metrics

For wireless mesh networks, various routing metrics have been designed to share radio resources efficiently. Although there is lots of work aimed to compare performance of these metrics, there is not a satisfactory study that can explain differences between metrics precisely.

Low-delay and presence of demand for high level communication have caused WMNs to be an alternative solution against to 3G cellular systems and WLANs [9].

While WMNs provide high service range, they also allow low-cost setup. Existing setups [10;11] show the high potential of commercial value of WMNs.

Nevertheless, even all of these technologies and probability of data transmission over multi-channels, transmission rate of WMNs is limited. Thus, to provide high demand of customers for quality of service (QoS), resource management and service providing mechanisms should be developed.

Most used routing metrics can be defined like below:

- **Hop Count:** Hop count is the most used metric in wireless multihop networks. Selected path is the one with minimum number of links between a source and destination. This metric is very popular in ad hoc networks, because it uses route length as criteria, thus computation is simple. On the other hand, this metric could fail in specific wireless mediums and does not count in congestion caused by sharing of the transmission medium.
- **Blocking Metric:** Blocking metric has some advantages like simplicity, not having any additional cost except storing neighbors' information. However, this metric does not indicate any characteristic that considers link capacity or traffic flow, and just emphasizes interference problem non-exhaustively. Due to all of these reasons, blocking metric has a little improvement over hop count.

- **Expected Transmission Count (ETX):** ETX is the transmission count for delivering a packet over a wireless link successfully [12]. ETX of a path is the sum of ETXs of all links of this path. Let p_f and p_r be forward and reverse direction packet loss probabilities respectively.

Unsuccessful transmission probability, p is shown in Eqn(1):

$$p = 1-(1-p_r)(1-p_f) \qquad (1)$$

Therefore, the expected number of transmissions to successfully deliver a packet in 1 hop can be expressed as in Eqn(2):

$$ETX = \sum_{k=1}^{\infty} kp^k (1-p)^{k-1} = \frac{1}{1-p} \qquad (2)$$

The delivery ratios are measured using 134-byte probe packets. One probe packet is sent every 7 second (set to 1 sec in the experiments). The packet loss ratio is computed by counting the number of probe packets received over a predetermined period of time (10 seconds).

ETX supports routes with higher load and less hop count because longer routes have lower load by reason of self-interference. Beside, ETX does not count the differences between transmission levels.

If a packet sender notices that channel is busy, then it delays sending of packet and does not allow for catching interference on the transmission medium.

Inasmuch as transmission rate of control packets is generally low, ETX does not give robust info about how busy the link actually is. In addition to this, it does not have information for efficient link sharing.

- **Expected Transmission Time (ETT):** ETT is a metric that has been designed over ETX by adding bandwidth to ETX compute. ETT is an improvement over ETX as it includes the bandwidth in its computation [13]. Let S and B be the packet size and the bandwidth of the link considered respectively. Then ETT is computed as in Eqn(3):

$$ETT = ETX \frac{S}{B} \qquad (3)$$

- **Weighted Cumulative ETT (WCETT) :**Similar to ETX, the expected transmission time of a path is computed as the sum of the links' ETT along the path. ETT later was improved by proposing Weighted Cumulative ETT (WCETT)[13]. This metric was designed to favor channel diverse paths. For a path p, WCETT is defined as in Eqn(4):

$$WCETT(p) = (1-\beta) \sum_{link l \in p} ETT_i + \beta \max_{1 \le j \le k} X_j \qquad (4)$$

Whereβ is a tunable parameter less than 1 and X represents the number of times channel j is used along path p.

Nonetheless, this metric still suffers from the same limitations as ETX/ETT by not estimating the effective link share and does not completely capture inter-flow interference.

- **Modified Expected Number of Transmissions (mETX):** [14] proposed an enhancement over ETX based on the observation that ETX does not take the channel variability into account and only considers the average channel behavior. The authors therefore defined mETX as in Eqn(5):

$$mETX = \exp(\mu_{\Sigma} + \frac{1}{2}\sigma_{\Sigma}^{2}) \qquad (5)$$

Where σ_{Σ}^{2} represents the average and the variability of the error probability.The main challenge in the implementation of this metric is to properly model and quantify the variability of the transmission channel.

- **Metric of Interference and Channel-Switching (MIC):** [15] has been designed to improve over WCETT by capturing more information on the effective link share. For a network composed of N nodes and a path p, MIC averages the time to transmit on a particular link over the minimum time to transmit over all the existing links. Similarly to WCETT, MIC adds a term to account for channel diversity called Channel Switching Cost (CSC). Calculation of MIC is shown in Eqn(6).

$$MIC(p) = \frac{1}{N\,x\,\min(ETT)} \sum_{link\ l \in p} IRU_l + \sum_{node\ i \in p} CSC_i \qquad (6)$$

min(ETT) represents the smallest ETT in the network and IRU_l represents the interference-aware resource usage defined as shown in Eqn(7) and Eqn(8) [10]:

$$IRU_l = N_l\, x\, ETT_l \qquad (7)$$

$$CSC_i = \begin{cases} w_1, & if\ CH(prev(i)) \neq CH(i) \\ w_2, & if\ CH(prev(i)) \equiv CH(i) \end{cases} \qquad (8)$$

$$0 \le w_1 < w_2$$

N_l is the number of nodes link 1 is interfering with, ETT_l is the expected transmission time on link 1, CH(i) is the channel assignment of node i and prev(i) represents the node before node i along path p. IRU_l can therefore be interpreted as the total channel time consumed by link 1. CSC is a weight allocated to a link as a function of the channel used by the link preceding the link considered on a particular path. If both links use the same channel, a greater weight is assigned to the link.

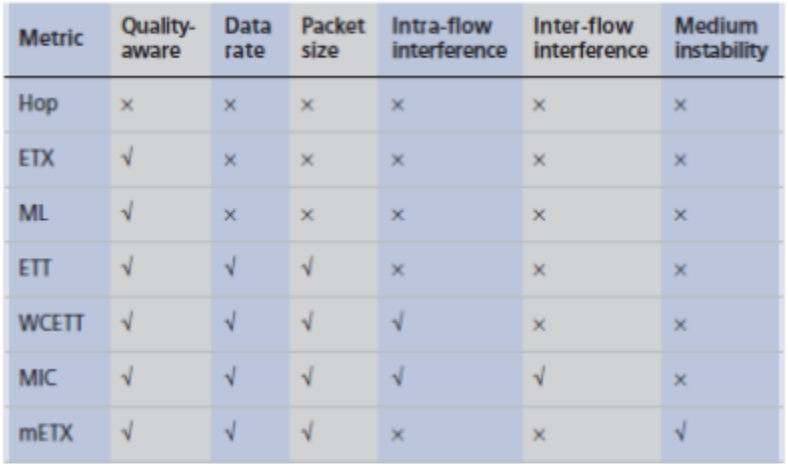
This metric presents some major drawbacks in terms of implementations [10]. First the overhead required to maintain up-to-date information of the ETT for each link can significantly affect the network performance depending on the traffic loads. Second, this metric assumes that all the links located in the collision domain of a particular link contribute to the same level of interference, which is oblivious of the differences of traffic loads at each node.

- **Network Allocation Vector Count (NAVC):** NAVC [16] essentially cares for the interflow interference by averaging the values of the Network Allocation Vector experienced by a node along a link for a given observation period. According to the value obtained, a level of congestion is attributed to the node. During the route discovery process, two parameters, heavy-node-number and navsum, are maintained. Upon reception of a ROUTE REQUEST packet, a node has three options depending on the value of the measured NAVC [10].
    1. If NAVC > 0.65: increase heavy node-number by 1 and add the square of NAVC to navsum;
    2. If 0.25 < NAVC < 0.65: increase navsum by thesquare of NAVC;
    3. If NAVC < 0.25: do nothing.

Then the cost of a path consists of the sum of the heavy-node-number of each node along the path and the sum of the nav-sum. Priorities are distributed to paths first according to heavy-node number then nav-sum.
In Table 1 [17] , the main characteristics of routing

metrics mentioned above are described.

Table 1: The characteristics of routing metrics.



Metric	Quality-aware	Data rate	Packet size	Intra-flow interference	Inter-flow interference	Medium instability
Hop	×	×	×	×	×	×
ETX	√	×	×	×	×	×
ML	√	×	×	×	×	×
ETT	√	√	√	×	×	×
WCETT	√	√	√	√	×	×
MIC	√	√	√	√	√	×
mETX	√	√	√	×	×	√

IV.II. Routing Protocols

Ad hoc routing protocols generally are categorized as proactive, reactive and hybrid. Proactive strategy works like classical routing of wired networks. Routers makes sure that at least one path reaches to any destination. On the other hand, reactive protocols allocate the path if only there is a packet that is to be sent to the destination. If a node does not have a packet to send to a certain destination, then node does not request a path to this destination.

Many of WMN routing protocols use similar strategies that are adopted from ad hoc networks. A classification of four main categories for WMNs [17] can be given as: ad-hoc based, controlled flooding, traffic aware (tree-based) and opportunistic protocols.

- **Ad-hoc Based WMN Routing Protocols**

WMN ad-hoc based protocols adapt ad-hoc routing protocols to deal with link quality variations. Routers progressively update link metrics and disseminate them to other routers.

The Link Quality Source Routing (LQSR) protocol combines link-state proactive routing and reactive strategy from ad hoc networks [18]. As a link-state protocol, LQSR uses the overall view of network for computing shortest paths.

SrcRR is another ad-hoc based protocol [19]. SrcRR uses a discovery procedure to update the routing information of traversed links. This method is like reactive protocol. But it does not need all view of the network to compute routes. Both SrcRR and LQSR perform route discovery procedure by using source routing and ETX.

The Multi Radio LQSR (MR-LQSR) is adapted from LQSR to operate over multichannel and multiradio by using WCETT metric [18]. Although WCETT does not assure paths with minimum costs, MR-LQSR is loop-free due to usage of source routing.

- **Controlled Flooding WMN Routing Protocols**

Controlled flooding protocols are designed to reduce control cost. By comparison with classical flooding, two main approaches which reduce routing cost, has been proposed as seen in Figure 6a [17]. In temporal flooding (Figure 6b), frequency is defined according to distance to router. Besides, by using spatial flooding (Figure 6c), far nodes get less certain and less detailed information from source. The main idea is that flooding network is inefficient as lots of connection in wireless networks occurs between close nodes. Thus, it is not necessary to send control packets to distant nodes as frequently as close nodes. Another way of reducing overhead is limiting the number of nodes which are responsible for flooding.

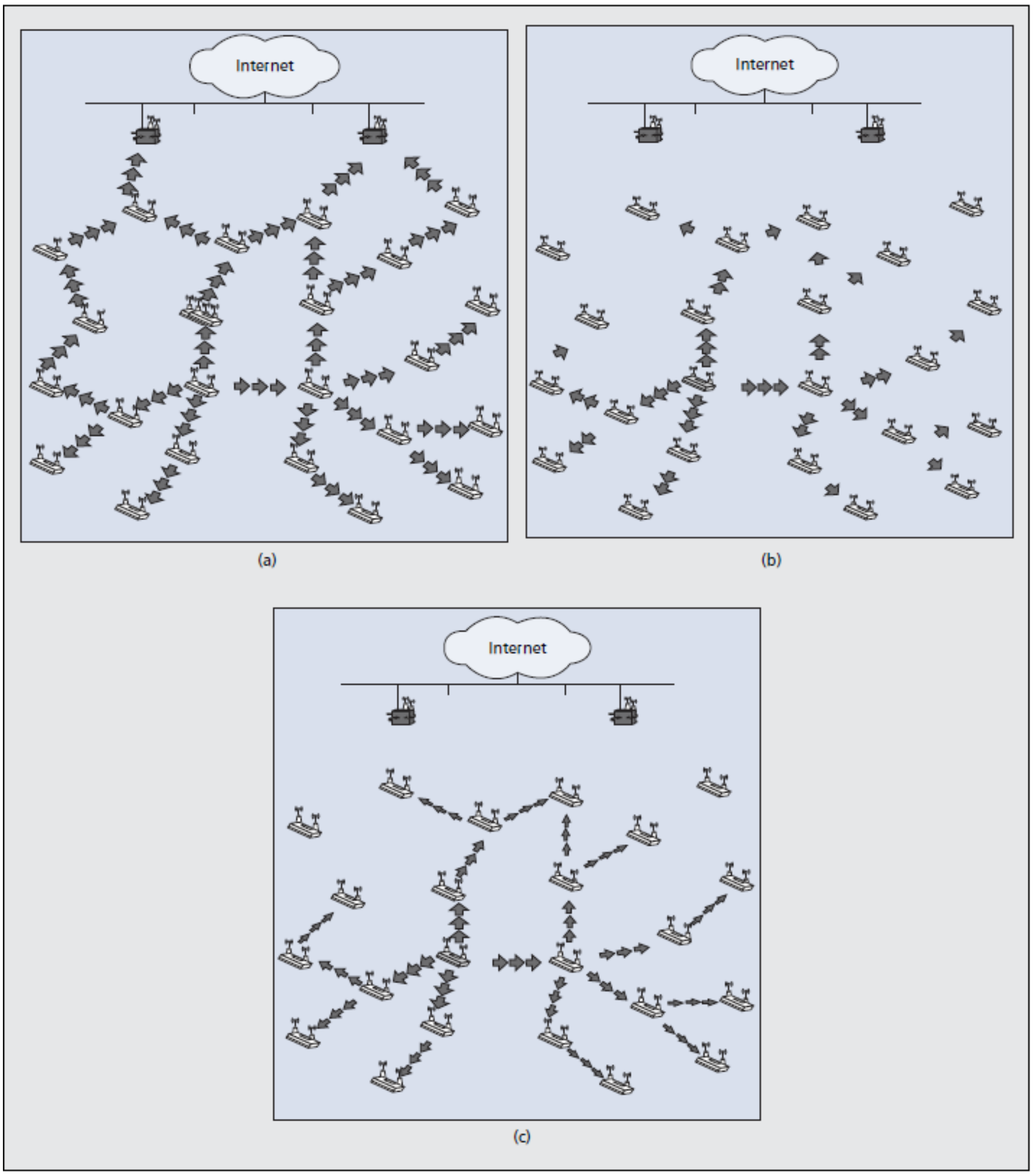


Fig. 6: Flooding Types: a) Classical, b) Temporal, c) Spatial.

The Localized On-Demand Link State (LOLS) protocol assigns a long-term and a short-term cost to links [20]. Long-term cost defines usual costs while short-term cost defines current costs. To reduce control overhead, short-term costs are sent to neighbors frequently as long-term costs are sent in long periods. LOLS computes path by using ETX and ETT.

Mobile Mesh Routing Protocol (MMRP) assigns an age to routing protocols, like open shortest path first (OSPF) protocol. Whenever a message is sent by a node, the time that is needed to transmit message, is subtracted from age. It is provided to drop a packet and resend when packet's time becomes zero. MMRP does not define a routing metric.

Optimized Link State Routing (OLSR) is another example of controlled flooding (RFC 3626) [17]. OLSR has been adapted to use ETX as a WMN metric. Every node choses its own MPRs which is the combination of nodes that is responsible for transmitting received routing information from fraction nodes. Each node constructs an MPR set with the minimum number of one-hop neighbors required to reach all two-hop neighbors.

- **Traffic-Aware WMN Routing Protocols**

Traffic-aware (or tree-based) protocols consider WMNs' general traffic matrix [17].

Ad-hoc on demand distance vector-spanning tree (AODV-ST) [21] adapts AODV from ad-hoc networks. On AODV-ST, the gateway requests current path info from every node in the network to

update routing table.
Raniwala and Chiueh propose a routing algorithm stand up to spanning tree used in wired networks [22].Route maintenance is done with *join* and *leave* requests. This protocol uses the hop metric and other metrics for load balancing.

- **Opportunistic WMN Routing Protocols**

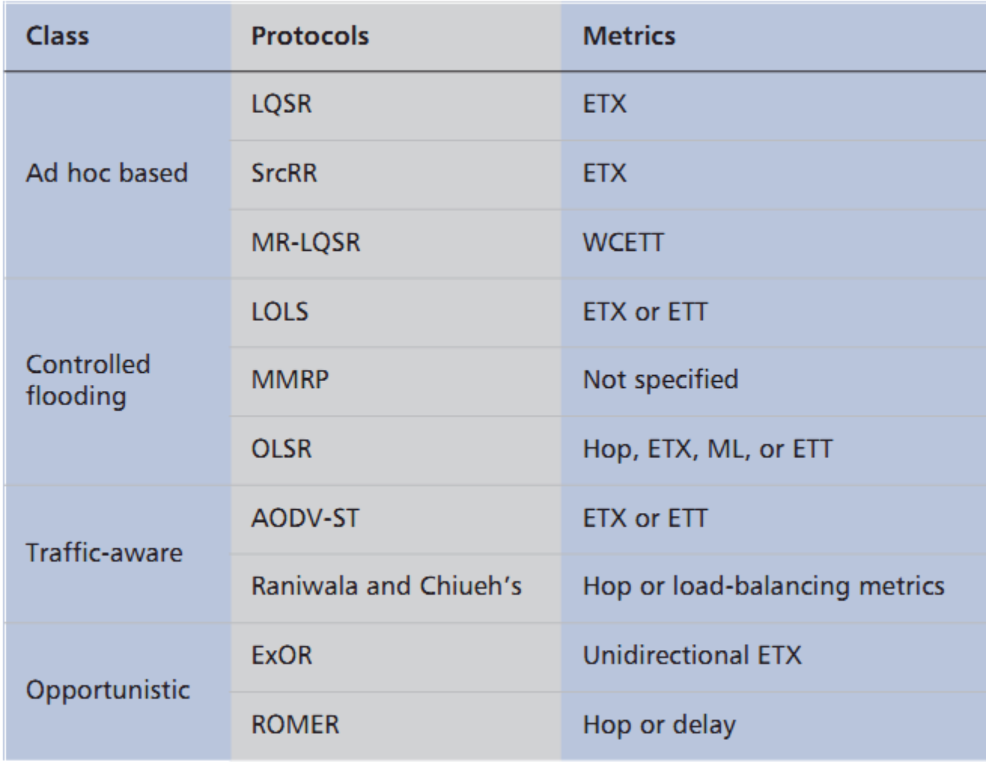
Opportunistic protocols promote routing based on cooperative variety schemes. In the case of link failures, successful link layer retransmissions are implemented until successful receiving on the neighbor reached at the next hop or maximum number of link layer retransmission is acquired. These protocols guarantee data to be transmitted somewhere that can be reached at least by one hop.

Extremely Opportunistic Routing (ExOR) protocol combines routing with MAC layer functionality [23]. Routers send broadcast packets as stacks that do not include the former route computing. Due to this stack structure, protocol cost can be reduced. Moreover, broadcasting data packets enhance reliability, because in order to hear a transmission just an intermediate router is needed. Source radio constructs a list of radios that might be able to forward data from itself to the destination. The radios' IDs are placed in a list sorted by distance to the destination, from closest to furthest. The destination radio is at the head of the list. Also, the source radio starts a list of the packets in the batch in order to measure packets' progress. This "batch map" is an array of radio IDs, one per packet. Each radio ID denotes the radio that transmitted that packet, and was closest to the destination radio. Each data packet has the list of radios, and packets placed in the front. The list saves space in each packet by using radio IDs rather than IP addresses. Then, the source radio broadcasts the first batch of data packets. It sets a timer. Radios that receive a packet but are not in the list in the packet ignore the data packets. These radios throw away the packets as soon as the packets are received. Radios that are in the packet's list of radios save the data packets that are received. They also update their batch map. When a radio times out, it transmits the packets that no radio closer to the destination has retransmitted. These packets include the radio's best available information about the progress of the packets in the batch (i.e. its batch map). In particular, each packet's batch map contains the retransmitter's radio ID for each packet that it retransmits. When a radio receives a packet sent from a radio that is closer to the destination, it erases its own copy of that packet. There's no need for it to retransmit that packet. However, it also updates its batch map about the progress of the packets in the batch. In this way, the information about the progress of the packets flows backward toward the source as radios further from the destination update their batch maps by eavesdropping on retransmissions.

Resilient Opportunistic Mesh Routing Protocol (ROMER), ROMER balances between long-term route stability and short-term opportunistic performance [24]. It builds a runtime, forwarding mesh on a per-packet basis that offers a set of candidate routes. The actual forwarding path by each packet opportunistically adapts to the dynamic channel condition and exploits the highest rate wireless channels at the time. To improve resilience against lossy links, ROMER delivers redundant data copies in a controlled and randomized manner over the candidate forwarding mesh. ROMER uses opportunistic, forwarding mesh adjusted on a packet basis to ensure robustness and high throughput. The mesh is centered around the long-term stable, minimum-cost, but opportunistically expands or shrinks at the runtime to exploit the highest-quality, best-rate links enabled by the physical-layer multirate options. The actual forwarding routes select the high-rate links out of the candidate routes offered by the mesh. The actual forwarding routes are also randomized to deliver redundant data copies in a controlled manner to ensure resiliency against lossy links and transient node outages. In short, ROMER takes a two-tier routing approach and balances between long-term optimality and short-term opportunistic gain. In contrast to ExOR, ROMER implements packet based communication to suit medium changes faster.

In Table 2 [17] WMN routing protocols and metrics used are shown.

Table 2: Classification of WMN Routing Protocols and Metrics.



Class	Protocols	Metrics
Ad hoc based	LQSR	ETX
	SrcRR	ETX
	MR-LQSR	WCETT
Controlled flooding	LOLS	ETX or ETT
	MMRP	Not specified
	OLSR	Hop, ETX, ML, or ETT
Traffic-aware	AODV-ST	ETX or ETT
	Raniwala and Chiueh's	Hop or load-balancing metrics
Opportunistic	ExOR	Unidirectional ETX
	ROMER	Hop or delay

IV.III. Assessment of Network Performance According to Metrics

According to recently proposed simulation works [10;14;17], effects of metrics on network performance is categorized below.

- **Hop Count**

The most important thing for minimum loss (ML) metric is link quality, for this reason it choses paths that have maximum number of hop counts.

ETX and ETT metrics choose paths that have the same number of hop counts without choosing same paths. Results show consistency with physical distances between nodes and their link qualities.

- **Packet Loss Rate**

On packet transmission process, in case of using hop count metric, while distance to destination node increases, high packet loss rates are obtained. The reason for this is that hop count metric does not consider link quality and it transmits packets over long, noisy links.

On the other hand, ETT and ETX result low level packet loss rate independent of distance.

ML metric has the best performance among other metrics, because its design is based on the selection of low level lossy links.

- **Network Delay**

According to average round trip time of packets from a source to a destination, using hop count metric causes increase in network delay. The main reason of this is that, much as links have less number of hop count are used, lossy structure of these links causes an increase in layer 2 retransmission count. As a result, longer delays occur on layer 3 packets. For ETX less than 150 ms, for ML 75 ms and for ETT 35 ms delays can be monitored.

- **Load**

Typical ETT, ETX and ML metrics by comparison with hop count metric, choose routes that have less number of hop count. On multihop transmissions in the shared medium, every additional hop causes increase of collision and conflict probability, and also it affects load negatively.

For short ranges, all of these metrics can reach high load rates. As soon as distance increases, hop count metric's performance decreases visibly while the other metrics give a satisfactory load level.

V. CONCLUSION

Because of the high demand for communication at everywhere and wish for guarantee of QoS, next generation technologies have emerged with their easy deployment, low-cost and versatility functionalities. Wireless mesh networks has been proposed as a solution that offers extended network coverage over multihop communication. Some characteristic properties of WMNs separate them from traditional wired and wireless networks and thus, new source management techniques are required.

Routing process on multihop wireless networks is a problematic research topic due to self-interference and interference of simultaneous transmissions. Besides, medium quality is another trigger factor for retransmissions which effect network performance.

A routing algorithm which combines aforementioned parameters to compute routes is required to overcome the problems. However, depending on the network configuration, a metric like hop count shows performance as good as or better than sophisticated metrics like ETX or MIC.

In the first instance, it is thought that ETX or MIC shows better performances because they try to prevent interference of simultaneous transmissions. But all metrics except NAVC can reach same performance level on a single channel system with respect to packet loss and end-to-end delay. There can be lots of reasons for that. Firstly, shorter paths are affected by self-interference and link/node interference although they are prone to passing over jammed routes. Secondly, the well-known problem of 802.11 is that it supports shortest paths. Thus, flows that are sent over longer paths are more susceptible to suffer from starvation. On the other hand, mETX and MIC shows better performance than hop count and blocking metric by forwarding packets over less congested areas. So, they provide a better traffic distribution.

General opinion of previous works is that hop count metric gives poor results, because this metric does not consider link quality. Besides, ML, ETX and ETT show better performance in the point of the view link quality.

Design of WMNs comes with a lot of problems. These problems can vary from routing metrics to security. Another way to increase routing efficiency is cross-layer design. To overcome this issue, reflecting PHY-layer changes or using proper radio spectrum is given as solution.

Existing applications and protocols evaluate metrics on single channel systems rather than multi-channel systems. But while passing from theory to reality, multi-channel structure must be considered and the works which overcome the deficiencies must be focused on.

Wireless Mesh Networks have capacity to answer lots of problems by their selves. This network technology which performs all of features like speed, security and accessibility from far and near, seems to be future solution of nowadays by correcting the deficiencies and doing necessary researches.

VI. REFERENCES

[1] Elizabeth M. Royer, Chai-KeongToh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April, 1999.

[2] W. Zhang, Z. Wang, S. K. Das, and M. Hassan, “Security Issues in Wireless Mesh Networks,” In Book Wireless Mesh Networks: Architectures and protocols. New York: Springer, 2008.

[3] AKYILDIZ I.F., WANG X., 2009, Wireless Mesh Networks, WILEY, United Kingdom, 978-0-470-032565.

[4] METHLEY S., 2009, Essentials of Wireless Mesh Networking, CAMBRIDGE, New York, 978-0-511-58070-3

[5] M.S.Aswall, Paramjeet Rawat, Tarun Kumar, “Threats and Vulnerabilities in Wireless Mesh Networks”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[6] Mihail L. Sichitiu, “Wireless Mesh Networks: Opportunities and Challenges”, Wireless World Congress, May 2005.

[7] Philip Whitehead, “Mesh Networks; a new Architecture for Broadband Wireless Access Systems”, IEEE Radio and Wireless Conference,September, 2000.

[8] Eng Chun; Lv Qin, LiuYong, Shi MeiLin, “Routing Protocols Overview and Design Issues for Self- Organized Network”, Communication Technology Proceedings, 2000. WCC - ICCT 2000, August, 2000.

[9] John Bellardo and Stefan Savage. “802.11 Denial of- Service Attacks: Real Vulnerabilities and Practical Solutions”. In Proceedings of the USENIX Security Symposium, pages 15–27, August 2003.

[10] S. Waharte, B. Ishibashi, R. Boutaba, “Performance Study of Wireless Mesh Networks Routing Metrics”, Computer Systems and Applications, April, 2008.

[11] K. Rayner. Mesh wireless networking. Communications Engineer, 1(5):4447,Oct.-Nov. 2003.

[12] H.-Y. Wei, S. Ganguly, R. Izmailov, and Z. Haas. Interference-aware IEEE 802.16 WiMax mesh networks. In Proceedings of the IEEE

Vehicular Technology Conference (VTC), 2004.

[13] D. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing.In Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom), 2003.

[14] R. Draves, J. Padhye, and B. Zill.Comparison of routing metrics for static multi-hop wireless networks.In Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM), August 2004.

[15] Y. Yang, J. Wang, and R. Kravets.Designing routingmetrics for mesh networks. In Proceedings of the 1st IEEE Workshop on Wireless Mesh Networks (WiMesh),2005.

[16] C.E. Koskal and H. Balakrishnan. Quality-aware routing metrics for time-varying wireless mesh networks. IEEE Journal on Selected Areas in Communications, 24(11):1984-1994, November 2006.

[17] Miguel Elias M. Campista, Pedro Miguel Esposito, Igor M. Moraes, Luís Henrique M. K. Costa, Otto Carlos, Diego G. Passos, CélioVinicius N. de Albuquerque, Débora Christina M. Saade, Marcelo G. Rubinstein, “Routing Metrics and Protocols for Wireless Mesh Networks”, IEEE Network,2008.

[18] R. Draves, J. Padhye, and B. Zill, “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks,” ACM MobiCom, Sept. 2004, pp. 114–28.

[19] D. S. J. de Couto, “High-Throughput Routing for Multi-Hop Wireless Networks,” Ph.D. diss., MIT, 2004.

[20] S. Nelakuditi et al., “Blacklist-Aided Forwarding in Static Multihop Wireless Networks,” IEEE SECON ’05, Sept. 2005, pp. 252–62.

[21] K. N. Ramachandran et al., “On the Design and Implementation of Infrastructure Mesh Networks,” IEEE Wksp. Wireless Mesh Networks, Sept. 2005.

[22] A. Raniwala and T.-C.Chiueh, “Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network,” IEEE INFOCOM, Mar. 2005, pp. 2223–34.

[23] S. Biswas and R. Morris, “ExOR : Opportunistic Multi-Hop Routing for Wireless Networks,” ACM SIGCOMM, Aug. 2005, pp. 133–44.

[24] Y. Yuan et al., “ROMER: Resilient Opportunistic Mesh Routing for Wireless Mesh Networks,” IEEE Wksp. Wireless Mesh Networks, Sept. 2005.