Routing for Wireless Multi Hop Networks – Unifying and Distinguishing Features

Technical Report 2011-583

Sherin Abdel Hamid
Hossam Hassanein
Glen Takahara

Telecommunications Research Lab (TRL)

School of Computing

Queen's University

Kingston, Ontario, Canada, K7L 3N6

December 2011

Abstract

In a wireless multi-hop network, one of the important challenges is how to route packets efficiently. The availability of many intermediate nodes between a source and a destination results in having many optional paths/routes to follow. The challenge is to pick an optimal path that satisfies the needed performance requirements - this is the responsibility of the routing protocol. There are four wireless network paradigms under the category of wireless multi-hop networks: Mobile Ad-Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Vehicular Ad-Hoc Networks (VANETs). In these four network paradigms, routing plays a vital and critical role and is considered one of the most important design elements. Being categorized as wireless multi-hop networks, the four aforementioned network paradigms share some commonalities in terms of their routing functions. However, as each of these network paradigms has its own unique characteristics and environment/application needs, each has some distinct aspects that distinguish its routing approaches from others. The focus of this depth paper is showing the unifications and distinctions of routing functions for the four multi-hop networks. In addition, we propose a generic routing model that can be the foundation of the wireless multi-hop routing function and can be inherited by any wireless multi-hop routing protocol. As well, we present our view of the ideal wireless multi-hop routing protocol along with several open issues.

1 Introduction

Generally, wireless communication refers to the use of untethered communication (e.g. infrared, acoustic, or radio frequency signals) for sending and receiving data between devices equipped with wireless interfaces [1]. Since its introduction, wireless communication is considered a revolution for communication and networking technologies with the great advantages that it provides in comparison to its wired counterparts. With no wires needed for end-to-end communication, wireless communication provides flexible deployment and use, cost reduction, mobility, network scaling, and convenience for both users and service providers. Having such advantages comes at the price of some drawbacks and limitations due to the characteristics of wireless communication, among them:

- Due to the "broadcast" nature of wireless communication, devices are subject to interference with one another. Higher interference usually results in lower reliability of data transmission.
- Lower bandwidth and data rates compared to wired communication; which results in higher delay/jitter and longer connection setup.
- Highly dynamic network conditions due to interference, loss of signal power with distance and freedom of mobility [1].
- Fading due to obstacles and the "multipath effect".
- Frequency reuse due to limitation of bandwidth and spectrum.

One of the most prominent drawbacks is the limitation in transmission range due to the previously mentioned characteristics. Therefore, nodes using wireless communication can only communicate directly with nodes within their transmission range. There are two wireless communication setups sharing this feature:

1) Infrastructure-Based, where nodes communicate directly with an access point or base station that coordinates communication with other nodes,

2) Infrastructure-less or Ad-Hoc, where nodes communicate with one another without the aid of any coordinator or central controller.

In the ad-hoc mode, with the feature of limited transmission range, for a node to be able to communicate with another node out of its transmission range, it should depend on other intermediate nodes for packets to reach the intended destination. These intermediate nodes act as relays for the packet. This communication paradigm is known as "*multi-hop*" communication where a node can act as a source, a destination, or a relay.

Being an essential part of the 3rd layer of the protocol stack, routing plays a crucial role in the design of networks and networking-based applications. In a multi-hop network, for a packet to be sent from a source to a destination, it is the responsibility of the routing protocol to find a path between the two communicating nodes through intermediate nodes that act as relays for packets. Having multiple intermediate nodes results in having multiple potential paths to be followed. So, the role of a routing protocol is not only finding a path, but finding the optimal one that satisfies the needed performance requirements from a set of optional paths. Choosing an optimal path from a source to a destination can be done by optimizing one or more routing metrics (e.g. number of hops, distance, delay, packet loss rate, energy consumption, to name a few). The selection metric is chosen based on the application requirements (e.g. delay-sensitive, energy-critical, QoS-based). More details about routing metrics and their selection criteria will be discussed in the following sections.

Following the paradigm of multi-hop communication, four types of wireless networks can be classified as wireless multi-hop networks. These network paradigms are: Mobile Ad-Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Vehicular Ad-Hoc Networks (VANETs). Being multi-hop networks, these paradigms depend on a sequence of intermediate nodes for routing packets from a source to a destination. Although having this feature in common, routing characteristics and functionalities in these four network paradigms have some differences that resulted in having different routing protocols uniquely designed for each network paradigm. These differences emerge from having different characteristics and challenges that impose requirements on the routing functions for each paradigm. They all utilize multi-hopping but with different techniques for handling the different routing components.

The objective of this depth paper is to highlight the commonalities and distinguishing features of the aforementioned network paradigms. The remainder of this paper is organized as follows: in Section 2, we will discuss the unifying features and the basic networking components that the paradigms have in common. As well, some auxiliary components will be discussed. In addition, we will propose a generic routing model that can be a foundation of the wireless multi-hop routing function and be inherited by any wireless multi-hop routing protocol. In addition to showing the commonalities and unifying features, in Section 3 we will shed light on the distinguishing features for each network paradigm in terms of characteristics and challenges and their effects on the routing functions. Furthermore, we will provide an abstraction for the general routing functionalities for each of the four network paradigms. Section 4 will present open issues in the area of routing for wireless multi-hop networks, along with our view of the ideal wireless multi-hop routing protocol, and some concluding remarks.

2 Routing for Wireless Multi-Hop Networks – Unifying Features

2.1 Introduction

Routing is the main function of the network layer, the 3rd layer of the protocol stack, and its performance is highly affected by the lower layers, the physical and data link layers. In order for a routing protocol to be efficient and reliable, the protocol designer should consider the effects of the lower layers and provide mechanisms for handling these effects. For example, due to some features of the physical layer, the communication range of the devices/communicating nodes may be asymmetric. This means that if node A can send a message directly to node B, it is possible that node B cannot reply back directly to node A. These communication issues should be taken into account when designing a routing protocol. On the other hand, this kind of cross layer effects can be utilized to improve the performance of the routing protocol. For example, routing protocols that are designed to support QoS and low latency requirements must consider link qualities in choosing the optimal path among the set of available paths. These link quality measures can be obtained from the lower layers by passing parameters to the routing one. A designer of a routing protocol then should consider the functionalities of the lower layers, handle their affecting features, and utilize their measures, parameters, and, in some cases, their layer-specific packets.

For the wireless multi-hop networks: MANETs, WSNs, WMNs, and VANETS, there is no single wireless multi-hop routing protocol which can fit all. This is because each network paradigm has its own design challenges and needs. Yet, as they all are classified under the category of wireless multi-hop networks, they have some unifying features in common. There are some routing functionalities and components that are essential, and are common parts of any wireless multi-hop routing protocol.

In [2], M. J. Lee et al. proposed a taxonomy that can be followed in designing a wireless routing protocol. They propose breaking down the wireless routing protocol and functions into multiple smaller components. Some of these components are core ones that should be a part of any wireless routing protocol and others are auxiliary that can be included only when needed by the application requirements. Following this component approach, in the following sub-section, we will provide a detailed discussion of the routing components showing the core and auxiliary ones and when these auxiliary ones may be needed.

2.2 Routing Components – An Exhaustive View

By breaking down the wireless routing protocol into smaller components, we can analyze the components that should be included in any wireless multi-hop routing protocol and show the interacting behavior between them. The behavior of these basic components can be tailored to different application profiles and needs, while keeping and maintaining the core functional behavior and goal [2]. To satisfy network and application specific needs, extra components can be added to the routing protocol to control its behavior and maintain its performance as needed and specified by the application and network paradigm. Having the core components, a routing protocol can be easily extended to accommodate and support extra requirements, services and features by adding auxiliary components. In the two following sub-sections, we will discuss the core components that should be a part of the skeleton of any routing protocol and will shed light on some auxiliary components that may be used only based on the network and application needs.

2.2.1 Core Components

These components are considered basic blocks for any wireless routing protocol to provide its main function, getting a message from a source to a destination. These components are the route discovery, route selection, and route representation and data forwarding.

2.2.1.1 Route Discovery

Route discovery is the first stage of the function of any wireless routing protocol. Route discovery is the process of finding a route/set of potential routes between a source and an intended destination. The process of finding a route can be classified into three categories *proactive, reactive* or *hybrid*.

Proactive route discovery, also known as **table-driven** route discovery, depends on use of up-to-date routing information about the whole network to find a path from any source to any destination in the network. This routing information is exchanged among nodes either periodically or upon the occurrence of any change in the network topology. This information is kept at each node in a routing table. This type of route discovery pre-determines routes between any two nodes irrespective of the need for such routes. When a node has a packet to be sent, it does not need to wait for a route to be discovered. It consults its routing table, gets the up-to-date recorded route, then sends the packet without incurring a delay for the route to be discovered - the route is discovered a priori.

There are two sub-categories under the proactive routing category: Distance Vector (DV) and Link State (LS). They differ in how the network topology information is spread. These techniques are borrowed from the wired networks but they can be modified to handle the characteristics of MANETs.

a. Distance Vector Proactive Routing

In DV route discovery, each node maintains a routing table where it stores information about all possible destinations, the next node to reach that destination, and the best known distance to reach the destination (distance can be defined as the number of hops).

These tables are updated by exchanging information with the neighbors. Each node periodically sends a vector to its direct neighbors carrying the information recorded in the routing table to maintain topology. The distance vector contains the destinations list and the cost (the distance) to reach each destination.

The basic distance vector routing works in theory but has a serious drawback in practice. It suffers from a severe problem known as "count-to-infinity" [3]. This happens as a result of the occurrence of routing loops; when X tells Y that it has a path somewhere, Y has no way of knowing whether it itself is on the path. This drawback is common in the DV routing technique, and all DV-based routing protocol designs should consider this issue and find a mechanism to avoid it.

b. Link State Proactive Routing

Distance vector routing was used in ARPANET until 1979, when it was replaced by link state routing. The objective of LS routing is to provide an alternative to DV that avoids routing loops and the subsequent "count-to-infinity" problem. LS overcomes this by maintaining global network topology information at each node.

In LS routing, each node periodically sends information about the cost to reach each of its direct neighbors and it includes this information in what is known as the link state packet. This link state packet is sent to all the other nodes in the network by flooding. Each node does the same link state flooding procedure and, eventually, each node will have link state packets from all other nodes, so each node will have information about the complete topology and costs of all the links in the network. The Dijkstra's algorithm [4] can be run locally to construct the shortest path to all possible destinations. The results of this algorithm can be stored in the routing tables for later use [3].

Although the LS routing avoids some problems with the DV routing, it has a problem with its storage requirements.

As an advantage, the proactive route discovery incurs almost no delay as routes are calculated in advance and are available in the routing table. However, it has a disadvantage that may hamper its use in large networks. It incurs an overhead related to the periodic routing updates which may cause congestion for the network when it has a large number of nodes. Therefore, in most cases, the proactive route discovery has problems with network scalability.

The ***reactive*** route discovery is also known as the **on-demand** route discovery. As the name implies, the route is discovered on demand and only when needed. When a source has a packet to be sent, it initiates a route discovery process to set up a path to the intended destination. Many approaches can be followed for path setup with the most common one is having the source node broadcast a route request packet carrying the destination address and asking for a route for that destination. When the route request reaches the destination or an intermediate node that knows a route to that destination, a route reply packet is sent back to the source carrying details about the discovered route.

Some protocols perform route discovery on the fly hop-by-hop. When a node receives a packet to be forwarded to another node, it decides to which neighbor it should forward this packet. This type of routing is known as *self-routing* and it falls under the category of reactive routing as the route is established on demand. An example of this type of routing is the geographical routing where a node picks the next hop, based on the locations of its neighbors and their distance to the destination. The *self-routing* based protocols usually require a form of *neighbor discovery* to know about the potential forwarding nodes that the current node will choose from to be the next-hop.

The reactive route discovery avoids the drawback of the proactive one by avoiding exchanging periodic routing updates, which reduces the traffic overhead. However, as the path is discovered only on-demand, this type of route discovery incurs a delay overhead and longer latency for route establishment.

The category of the ***hybrid*** route discovery depends on combining both the proactive and reactive techniques to make use of the advantages of both and mitigate their disadvantages. It tries to reduce the control overhead associated with the proactive route discovery and the delay incurred in the reactive one.

2.2.1.2 Route Selection

As an output of the route discovery stage, there will be a set of potential routes between a source and destination. It is the role of the route selection component to pick the optimal path from this set that satisfies the needed performance criteria. Most of the routing protocols are based on choosing only one path for delivering packets from a specific source to a specific destination; however, there are some protocols that rely on choosing multiple paths (*multipath routing*) [5] to provide redundancy and fault tolerance for the routing process.

For the proactive protocols, route selection is done implicitly with the route discovery stage. When the network topology information is shared and received by the nodes, they update the information in their routing tables accordingly; hence, routes available in the routing tables are the selected, best ones at that time.

Route selection in the reactive protocols is a stand-alone process. It can be handled by the source, the destination, or the intermediate nodes. In *destination-based route selection*, when the destination receives multiple route requests forwarded by multiple intermediate nodes, it can select the path to receive data through and sends the route reply along this path. The destination can pick the first path through which it received the first route request (the fastest one), or it can wait for a specific period of time, thereafter, if it has received many route requests, it can pick the optimal path according to some selection metrics, discussed later in this section.

In *source-based route selection*, the source node may receive multiple route replies from the destination (the destination replies to all route requests it receives) or from all intermediate nodes that know about a route to the intended destination. It is the responsibility of the source to pick a route from the set of routes extracted from the multiple route replies.

For the *intermediate-based route selection*, the intermediate nodes decide upon which route a packet should follow to reach a destination. They can either choose a route from a set of possible routes they keep for that destination[1], or, select a next hop on the fly. This type of route selection is involved in self-

[1] These routes may be discovered by them in a previous interaction with the destination or overheard from neighbors interacting with that destination.

routing protocols. Since the route is selected on a hop-by-hop basis, the intermediate nodes are involved in the route selection process when the packet is forwarded to any of them.

Whether route selection is done by source, destination, or intermediate nodes, the deciding node should depend on one or several metrics for the selection decision. Determination of which route metric to use is dependent on the application requirements and needs. The simplest route metric and the most popular one is the hop count. The path with the least hop count will be chosen to reduce the number of intermediate nodes involved in the routing process and so reduce the control overhead and contention level among nodes. Examples of other routing metrics include energy consumption level, residual energy of the next hop, QoS metrics (e.g. end-to-end delay/jitter, interference level, packet loss rate, link residual capacity, load balancing), link security level, and memory consumption. Some of these routing metrics require parameters related to the lower layers like the QoS-based link quality ones. These parameters can either be passed from the lower layers to the routing layer, or, in some protocols, this interaction with the lower layers is done in the form of cross-layer protocol design.

In short, how the route is selected is based on the application/network paradigm for which the protocol will be used. It is how the route will be selected that controls the performance of the routing protocol and whether it will satisfy the needs of the application or not.

2.2.1.3 Route Representation and Data Forwarding

After selecting a route, it should be stored to be followed for data transfer. We consider both route representation and data forwarding as a single component as they are highly integrated together and, in many protocols, they are done simultaneously. Route representation and data forwarding can follow one of two techniques: exact route and route guidance [2].

- **Exact Route**

In this technique, the sequence of intermediate nodes that a path should follow to reach a destination is represented explicitly. There are two approaches for using the exact route representation and forwarding. These approaches are *routing table* and *source routing*.

a) Routing Table

In this approach, each node keeps a routing table where it stores the next hop to reach potential destinations with one entry per destination. In the proactive protocols, this routing table contains information and next hops to all other potential destinations in the network. In the reactive protocols that make use of the routing table approach, they keep information about the destinations that they interacted with previously or those nodes that they overheard paths to them. Also, in these routing tables, they may keep information about nodes from which they received route requests or route replies for further relaying. When a packet is to be forwarded, the node looks up the routing table and gets the next hop to which it should forward the packet to reach the intended destination.

b) Source Routing

The idea of the source routing approach is to include the whole path that the packet should follow in the packet header, and when a node gets this packet, it can extract the next hop from the path included in the packet. This path is included by the source node before sending the packet. This approach encounters some problems especially with large networks; as the complete path is included in the packet header, this can be considered traffic overhead and a source for bandwidth wasting.

- **Route Guidance**

In route guidance-based protocols, the sequence of intermediate nodes is not explicitly described. The full path is not determined prior to sending the packet by the source, rather the path is formed on the fly (i.e. self-routing). As the route is not fully determined a priori, nodes cannot store information about the path itself but they may store information about how the next hop will be chosen or information that will be used for picking the next hop, this is what is called route guidance. The geographical routing protocols are examples of protocols that follow the route guidance technique. In these protocols, instead of keeping information about the path itself, nodes store the positions of their neighbors and pick the next hop on the fly based on the destination and their direct neighbors' positions [6].

The three aforementioned components are considered core ones that should be included in any wireless routing protocol. As mentioned above, their behavior can be tailored to meet the requirements of the network paradigm that the protocol is designed for as it will be shown in Section 3. In the following subsection, we will explore some of the auxiliary routing components that can be added to the core components to achieve a specific design goal.

2.2.2 Auxiliary Components

These components are not essential for all routing protocols but they can be added to improve the performance of a protocol or to make it meet the requirements and needs of a specific application or network paradigm. Examples of these components are route maintenance, route energy efficiency, and route security. Some of these components are discussed in the following.

2.2.2.1 Route Maintenance

The goal of the route maintenance component is to keep a route valid while in use and to handle possible failures. Route maintenance is needed by networks where links are prone to failure due to node mobility, for example. It is considered a crucial component in MANETs where nodes are highly mobile and the network topology encounters frequent dynamic changes. Route maintenance includes *route refreshing*, *route failure handling*, and *route invalidation* [2].

- **Route Refreshing**

Route refreshing aims at keeping the current routes valid by updating or using them only for the sake of refreshing. Route refreshing can be handled by one of three approaches depending on the category of the protocol: proactive, reactive, or hybrid. In the proactive protocols, route refreshing is done implicitly by having the nodes periodically or upon the occurrence of topology changes exchange network topology information and update the routing tables according to the current changes in the network. Therefore, in the proactive protocols, routes in the routing table are always the most up-to-date. In the reactive approach, routes are only touched on demand, so to keep routes usable and ensure their validity, nodes can refresh routes either by use of control packets (e.g. hello messages) or by using a data packet before the expiration of the route. Hybrid protocols and hybrid route refreshing combine both the proactive and reactive approaches.

- **Route Failure Handling**

In the reactive routing, when an intermediate node finds that the next hop is unreachable it tries one of two options: 1) to find an alternate path locally either by looking up its routing cache for an alternative or by initiating a route discovery process to replace the failing link with a valid one, or 2) to send a route error message to the source node with information about the failing link. The source node can also look up its route cache for a different route. If there is no alternative, it reinitiates the route discovery process while marking the failing part in order not to include it again.

In proactive routing, route failure is handled by route refreshing. As the routing tables have up-to-date routing information, route failure is handled by automatic updates.

In the hybrid protocols, it is a combination between the proactive and reactive route failure handling approaches.

- **Route Invalidation**

Route invalidation is the process of finding out stale routes and removing them from the routing tables and caches. The stale routes are distinguished and recognized by employing a lifetime period for each route, and if this route has not been refreshed during that period, it will be marked as expired and will be removed.

2.2.2.2 Route Energy Efficiency

As some of the wireless multi-hop networks are comprised of devices with limited resources, e.g. sensor nodes in WSNs, such networks have energy efficiency as one of the major design considerations that should be taken care of in any protocol designed for such networks including the routing ones. Routing protocols designed for such networks should include mechanisms to conserve node energy to prolong the lifetime of the nodes and of the network as a whole. Examples of such techniques are data aggregation, use of meta-data, load balancing, restricted flooding, use of energy-aware metrics, use of resource manager, and putting nodes into sleep mode.

- **Data Aggregation**

Data aggregation is one of the techniques that are highly utilized in the energy-efficient routing protocols because, when deployed, it has a great impact on the nodes residual energy and lifetime. The idea is that instead of sending redundant packets or packets that have a kind of correlation, these packets can be combined and aggregated together into only one packet. Reducing the number of transmitted packets leads to great conservation in nodes' energy.

- **Use of Meta-Data**

A number of protocols depend on sending meta-data that describes the actual data packets instead of sending the actual packets themselves. This technique is mainly used for advertising the actual data. Instead of sending long data packets to nodes that may not be interested in them, small meta-data is sent to advertise the acquired data packets and if a node shows its interest in such data, the complete data packet is sent to it afterwards.

- **Load Balancing**

Many protocols focus on balancing the traffic load among the nodes in order not to overload some nodes compared to others which may lead to depletion of these nodes' batteries and cause their failures. For example, in cluster-based routing protocols, if cluster formation is static and not changed throughout the network life, the nodes that act as clusterheads will burn their energy quickly, and after they die, all their members will be "headless" and therefore useless. This is because the role of being a clusterhead is energy consuming as the clusterhead has to be awake all the time, receive data from all of its cluster members, incur processing overhead for aggregating the data, and is responsible for the long-range transmissions to the data collector. To provide energy efficiency and balance energy consumption among the nodes, some routing protocols utilize dynamic clustering to rotate the role of being a clusterhead among the nodes.

- **Restricted Flooding**

When a packet needs to be broadcast (e.g. route request packets or data interests), some protocols make use of restricted flooding instead of flooding the packet to the whole network. For example, the packet can be sent to a group of nodes with higher probability to forward the packet or with wider coverage and view for the network. Another example is forwarding the packet to an area of interest instead of to the whole network (e.g. sending data interests geographically to the area of interest then flooding the interest only within this area).

- **Use of Energy-Aware Metrics**

When this technique is utilized, it can be considered a part of the route selection component. To conserve energy, the optimal route can be selected based on the included nodes' energy. The nodes' current energy consumption level or current residual energy can be used as the route selection metric.

- **Use of Resource Manager**

Some protocols add to the routing component a resource manager that monitors the energy level of the nodes and adjusts their operations based on some thresholds.

- **Putting Nodes into Sleep Mode**

As a common technique in most of the WSN protocols (either MAC, routing, or other layers protocols), putting nodes into sleep mode saves a significant amount of energy. In the sleep mode, only the processor works with very little portion of its capabilities (neither sensing nor transmissions are done). Once the node gets tasked or awakened, it works with all its capabilities.

2.3 Generic Routing Model

In this sub-section, we will present a generic routing model that can be used to form the foundation of a wireless multi-hop routing protocol. We will present the functionalities as blocks and methods that can be selectively utilized and combined together to form a wireless routing protocol suitable for any wireless multi-hop network. This generic model can be further extended and enhanced with auxiliary functionalities to meet specific requirements per network paradigm.

Each component will be presented with its own various functionalities that will be available to the protocol designer to choose from. The output and the input of each component will be shown to clarify the interactions between the various components. The proposed generic model is shown in Figure 1.

The route discovery component has five options/functions for the designer to choose from: ***1)*** proactive with distance vector, ***2)*** proactive with link state, ***3)*** reactive with deterministic routing, ***4)*** reactive with self-routing (which requires that each node discovers its neighbors, so, it calls the neighbor discovery function which feeds it with the neighbors list), and ***5)*** hybrid discovery.

The route selection component has three functions for the protocol designer to choose from: ***1)*** source-based selection, **2)** destination-based selection, and ***3)*** intermediate-based selection. The choice of which function to be used depends on the route discovery function that has been chosen (e.g. the reactive self-routing discovery requires the use of intermediate-based route selection).

Finally, the route representation and data forwarding component has three functions available for the designer's choice: ***1)*** representation and forwarding using exact route with routing tables, ***2)*** representation and forwarding using exact route with source routing, and ***3)*** representation and forwarding using route guidance. Again, the choice of the appropriate function strictly depends on the chosen discovery function (e.g. the reactive self-routing discovery requires the use of route guidance).

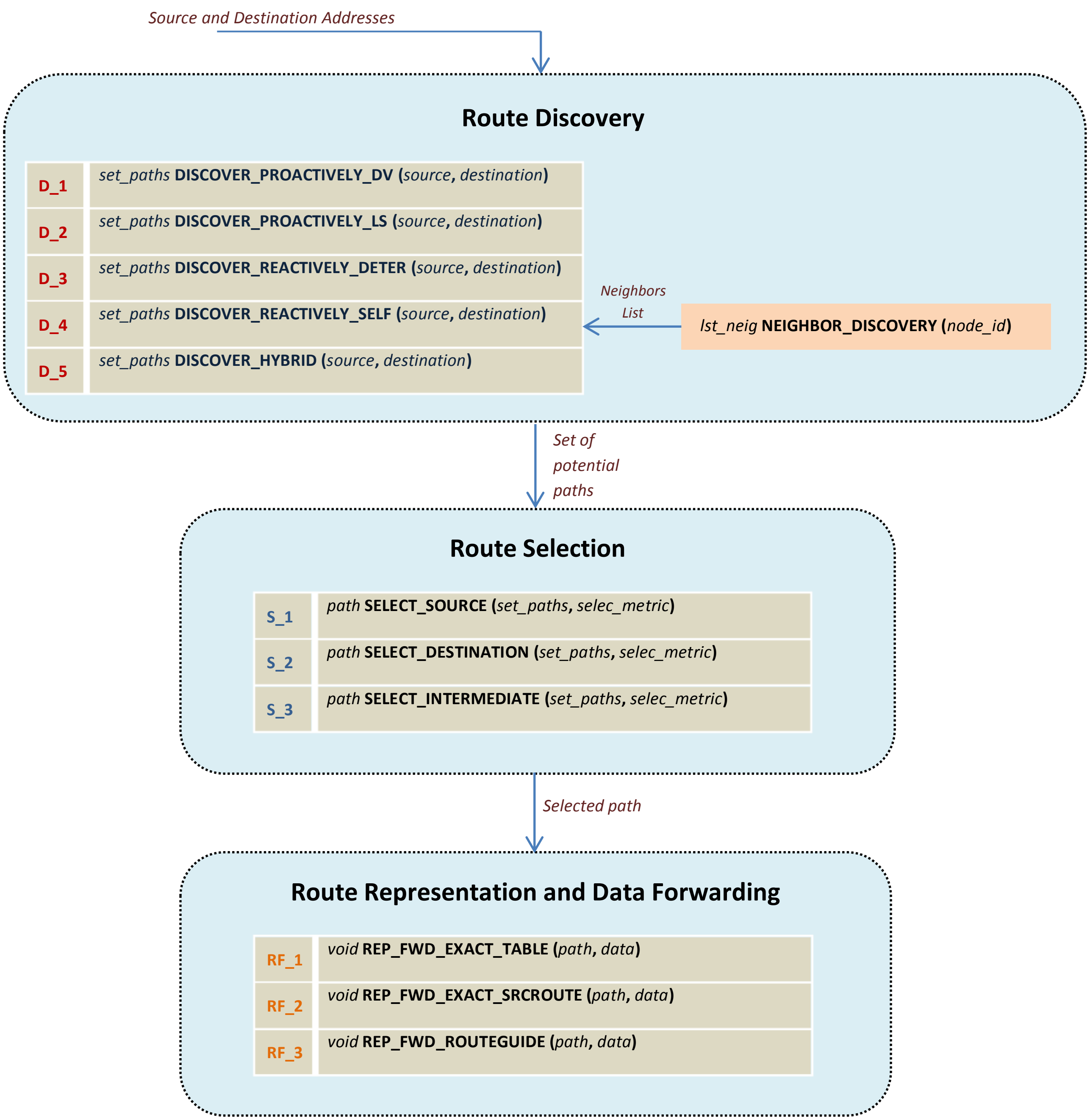

Figure 1 Generic Routing Model.

The following pseudo code shows the interaction and dependency of the route selection function and the route representation and data forwarding function to be chosen and the already chosen discovery function. For simplicity, we refer to the functions by codes – these codes are shown in Figure 1 next to their associated functions.

Pseudo code for choosing the route selection function and the route representation and data forwarding function based on the chosen discovery function

```
if D_1 or D_2 is chosen then
        choose S_1 and RF_1
else if D_3 is chosen then
        choose S_1 or S_2 or S_3   and   RF_1 or RF_2
else if D_4 is chosen then
        choose S_3 and RF_3
else if D_5 is chosen then
             // For the proactive part
             choose S_1 and RF_1
             and
              // For the reactive part
             if D_3 is chosen then
                  choose S_1 or S_2 or S_3   and   RF_1 or RF_2
             else if D_4 is chosen then
                  choose S_3 and RF_3
             end if
end if
```

By breaking down the functionalities into blocks and methods, the protocol designer can choose whatever functionalities are preferred and suitable for the intended paradigm and application. In addition, the designer can replace the chosen functionality of each component without having to redesign the whole protocol. The protocol design is based on a set of blocks that can be edited separately.

In implementing or modifying any of the functionalities, the protocol designer should consider including the scalability[2] and self-configuration[3] features as they are both basic features for all wireless multi-hop routing protocols.

3 Routing for Wireless Multi-Hop Networks – Distinguishing Features

As mentioned in section 1, there are four wireless networking paradigms - MANETs, WSNs, WMNs, and VANETs - that can be classified as wireless multi-hop networks as they all follow the pattern of wireless multi-hopping in sending packets among their networked nodes. Although these network paradigms have many characteristics in common, as each consists of different types of nodes and serves different applications, each has its own unique features, requirements, and design challenges that necessitate the need for a set of protocols designed specifically for each network paradigm. In this section, we will show the distinguishing characteristics and challenges for each of the four

[2] As it is wireless ad hoc so it is subject to increase in nodes' number

[3] As there is no central control available

aforementioned network paradigms, the most popular classification and schemes for each paradigm, and the core components and distinguishing functionalities of routing for each network paradigm.

3.1 Distinguishing Challenges and Characteristics

In this sub-section, we will discuss the features and challenges of each wireless multi-hop network paradigm for the sake of highlighting the differences and distinctions between all wireless multi-hop networks.

3.1.1 Mobile Ad-Hoc Networks

A **M**obile **A**d-Hoc **NET**work (MANET) is a collection of mobile nodes with wireless networking interfaces that form a temporary network without the aid of any infrastructure or central control [1] [7]. Examples of these mobile nodes include laptops, notebooks, palmtops, and PDAs. Nodes in a MANET are autonomous, self-organizing, self-configuring nodes that communicate in a multi-hop fashion and can move arbitrarily. Therefore, the network may experience rapid and unpredictable topology changes. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in the network.

MANETs originated from the Defense Advanced Research Projects Agency (DARPA) [8] Packet Radio Networks (PRENET) in the early 1970s. Being free of infrastructure, MANETs have many advantages such as ease of deployment, low cost, and high flexibility. Having these advantages, MANETs are appropriate for many commercial and industrial applications, for example, educational and file sharing purposes in conferences/meetings/lectures, emergency services, law enforcement operations, and home networking.

Due to the high importance of routing protocols in such dynamic networks, active research is carrying on and a lot of protocols have been proposed in the hot area of routing in MANETs. There are several design challenges that need to be considered in designing a routing protocol for MANETs:

a) Nodes Mobility

As the nodes are free to move, the network topology keeps changing. In addition to being either a source or a destination, nodes in MANETs are also working as routers for other nodes' transmissions, so the routing paths are always prone to failure and breakage. It is the responsibility of the routing protocol, besides discovering the route, to provide a recovery from such paths' failures. The routing protocol should have a route maintenance component to ensure that packets reach their destination in the shortest time even if the original path has been broken for some reason. The frequent change of network topology is considered the most significant and critical challenge for routing in the MANETs.

b) Resource Constraints

Nodes in MANETs are portable devices that are limited in their hardware resources. This imposes limitations on the complexity of the designed protocol.

c) Scalability

The routing protocol should provide an acceptable level of service even in the presence of a large number of nodes. Newly added nodes should be identified rapidly. In addition, the control packets must be utilized efficiently to deliver data packets, and be generated only when necessary in order not to cause network implosion when having a large number of nodes with frequent movements.

d) Lack of Infrastructure and Central Control

Being ad-hoc networks, MANETs should be self-organizing and configuring; there is no centralized administration entity to manage the operation of the different mobile nodes. The routing protocol should depend on distributed techniques for network configuration and assigning roles for the hierarchical structures (e.g. clustering).

e) Limited Bandwidth

As the nodes communicate using a wireless interface, the available bandwidth is limited. The routing protocol should enhance bandwidth utilization for better performance of the whole network. It should reduce the control packets as much as possible and minimize the data packets header size while keeping the protocol performance as efficient as possible.

All these design challenges should be taken into consideration in designing a routing protocol for MANETs with the main focus being on the most critical challenge, handling nodes mobility to maintain network connectivity.

3.1.2 Wireless Sensor Networks

A typical **W**ireless **S**ensor **N**etwork (WSN) consists of a large number of small, inexpensive, resource constrained sensor nodes that communicate wirelessly in a multi-hop network. These sensor nodes collaborate together to accomplish a common task and serve a certain application; for example, environment monitoring, battlefield surveillance, Intelligent Transportation Systems (ITS), home applications for domestic devices and users interaction, and industrial process control [9].

The sensor node basically consists of a sensing circuitry, a low-power embedded processor, small memory, radio transceiver, and a power source (usually is a small battery). There are other optional components that are application-dependent: a Global Positioning System (GPS), a mobilizer, and a power harvesting system. The sensing circuitry measures parameters from the surrounding environment and transforms them into electric signals. These signals are processed by the node for analysis and decision making purposes. The sensor node sends such sensed data, usually via a radio transmitter, with the aid of other nodes in the network through multi-hopping, to a data-collection station (a base station or a sink) that may be connected to a command center, either directly or through the internet.

Designing a routing protocol for WSNs is very challenging due to the WSN unique characteristics that distinguish this type of networks from any other wireless networks like MANETs. The design challenges in sensor networks involve the following main aspects:

a) Energy Constraints

Sensor nodes are restricted by their power supply as they are usually battery-powered, and in most applications it is difficult or infeasible to replace or recharge the batteries (e.g. in harsh environments). Having this power constraint, WSN applications and protocols should be designed to be as energy-efficient as possible to prolong both the nodes and network lifetime.

b) Limited Hardware Resources

The sensor node is also limited in its processing and storage capabilities, therefore WSN protocols should be as simple as possible and with low data storage requirements.

c) Dense Deployment

Sensor nodes are deployed in large numbers and can be several orders of magnitude higher than that in a MANET; there can be hundreds of thousands of nodes in the very large areas. The WSN protocol should work efficiently with this number of nodes and try to reduce the communication and control overhead that may cause network congestion and performance degradation.

d) Addressing Scheme

Due to the dense deployment in WSNs, it is not possible to build a global addressing scheme. Thus, the IP-based protocols may be not applicable to the WSNs. In addition, in WSNs, nodes collaborate together to achieve the overall application goals and perform the sensing tasks. In most cases, there is no interest in which nodes reported what; the interest is in the reported data itself regardless of which nodes they are sent from. The common addressing scheme in the WSN is the data-centric scheme which is based on the attribute-based addressing, where data is represented as attribute-value pairs that may be requested by queries sent by the base station or reported by the node in a time-based or event-based manner.

e) Scalability

Nodes are deployed densely in the WSN and more nodes may be added during the network operation to provide more coverage or accuracy. The protocol should accommodate all these nodes and be scalable to different network sizes.

f) Self-configuration

Being an ad-hoc network, it is the responsibility of the nodes to configure themselves on the fly once deployed and to organize themselves into a communication network. The routing protocol should provide distributed techniques to support this feature.

g) Fault Tolerance

Due to the limited resources, the sensor nodes are prone to failure; hardware failure or depleted batteries. This failure also may be due to environmental factors and unattended operations. The protocol for the WSN should be fault tolerant, handle the frequent topology changes, and utilize self-repairing and self-recovery mechanisms.

h) Data Redundancy

Due to the dense deployment of the sensor nodes, there are many nodes in an area of interest. The data sensed by these nodes are based on a common phenomenon and have some sort of correlation and redundancy. Exhausting the network with these redundant data causes problems with unneeded energy consumption and inefficient bandwidth utilization. On the other hand, this redundancy of data can be advantageous. By utilizing data aggregation techniques, this redundancy can be exploited by the routing protocol to decrease the number of transmissions; hence, improve the energy efficiency and the bandwidth utilization.

i) Diverse Applications

WSNs have a wide range of applications each with its own requirements. Therefore, there is no “one-for-all” protocol; the requirements of the data gathering applications are different from those of the critical events reporting. The protocol designers should develop the protocol in a way that satisfies the needs of the application and utilizes the resources efficiently.

Having all these unique challenges for WSNs forced the design of new routing protocols instead of using the existing protocols of MANETs. New protocols are needed to meet all these design challenges and provide the needed network performance. To make the WSN operational for several years, the energy efficiency should be the primary design goal in any WSN protocol.

3.1.3 Wireless Mesh Networks

Wireless **M**esh **N**etworks (WMNs) were proposed as an efficient technology to provide broadband access to users not in direct coverage of wired access points by extending the backhaul access using wireless communications. Isolated Local Area Networks (LANs) can be connected together and coverage can be extended without incurring the cost and inconvenience of deploying wired infrastructure.

A WMN is comprised of three tiers of networking components: 1) the mesh clients which are the user devices seeking access to the broadband network, 2) the wireless mesh routers (WMRs) that provide connectivity to the mesh clients and they are connected together in a multi-hop fashion for covering the access area, and 3) the gateways which are connected to the mesh routers and provide the last mile access to Internet. The general architecture is illustrated in Figure 2 . Only gateways need wired connection to the backhaul network. Being deployed in an ad-hoc fashion, wireless routers can be incrementally added to the network for further extension for the covered area as needed [10]. Except for the intra-mesh links which should be wireless, all other links can be either wired or wireless [11]. Clients can connect to the WMRs using any common network interface (e.g. 802.11, Ethernet, Bluetooth). WMRs can have multiple radio interfaces and can support multi-channel operation.

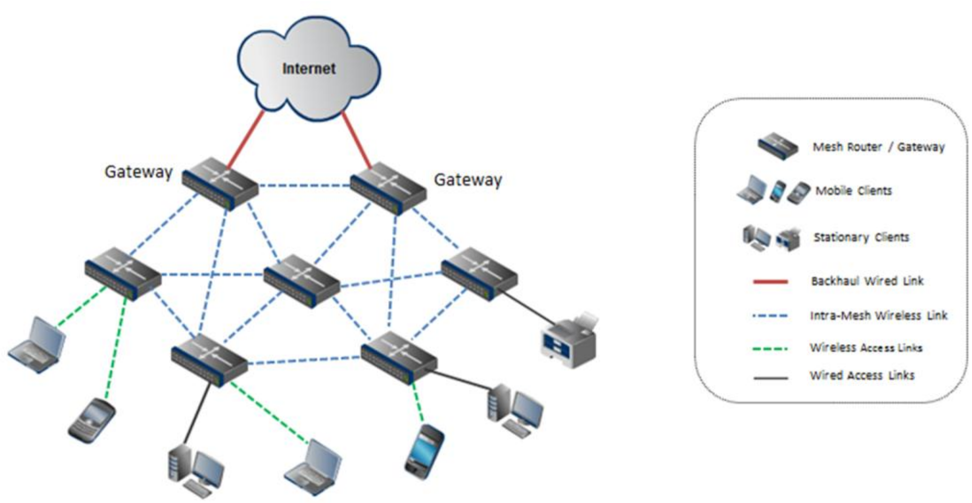

Figure 2 Architecture and components of a wireless mesh network.

The extended coverage capabilities provided by WMNs motivates a promising market and applications. The main objective for designing WMNs was to provide public Internet access for areas not covered by wired infrastructure. In addition to its main objective, WMNs can support other applications: communications for ITS, public safety, broadband home networking, community and neighbourhood networking, enterprise networking and building automation [10].

Communication in WMNs can be one of two patterns: communication between a mesh client and a gateway for the broadband access, or a communication between two mesh clients. In both cases, all transmissions are done via WMRs in a multi-hop fashion.

Routing for WMNs plays a crucial role for providing the WMN services with the required quality for users. WMNs have some unique characteristics that impose distinguishing challenges as well as improving opportunities for designing a WMN routing protocol. The most prominent ones are:

a) QoS Guarantee

As the main objective of the WMN is providing broadband services, routing for WMN should depend on the use of QoS and link quality metrics to satisfy the QoS requirements; minimize delay, provide real time communications, and balance the load between the multiple available paths.

b) Robust Coverage

To guarantee QoS and provide efficient services, the WMN should be more robust to network faults and link failures. Dead zones can be eliminated by adding mesh routers and by the proper placement of routers to avoid service disruptions. A WMN routing protocol should utilize the availability of multiple paths between the potential source-destination pairs. Such redundancy of communication paths can also impose challenges for the routing protocol represented in increased complexity for maintaining these paths.

c) Minimal Mobility

In the backbone WMN, WMRs are almost stationary. Having such static deployment, mobility support in WMN is not a major concern. This releases the burden and the complexity of handling mobility by the routing protocol. Also, being static, WMRs can be easily hooked up to permanent power supplies; hence, also no power constraints need to be handled by the routing protocol.

d) Multiple Radios

WMR may utilize multiple radios to increase capacity and improve QoS.[4] This feature dictates a unique challenge for the WMN routing protocols to handle. Also, having multiple interfaces requires cooperation between the routing layer and lower layers involving passing parameters among the layers or utilizing cross-layer functionalities.

e) Adaptive support for both mesh routers and clients

Most of the protocols are designed for the backbone mesh. New routing protocols are needed that include mechanisms for handling both the backbone WMNs and client WMNs features.

f) Scalability

QoS guarantee requires keeping the end-to-end delay as low as possible. Setting up a path in a very large network may incur a long delay. So, the routing protocols should be designed to be scalable and include mechanisms for keeping the end-to-end delay reasonable for all networks sizes.

These features and challenges uniquely distinguish the routing functions in WMNs. Some of them can be considered advantageous as they relax some constraints that are available in other network

[4] Utilizing multiple radios enables separation of two main types of traffic; while routing and configuration are performed between mesh routers on one radio, the access to the network by end users can be carried out on a different radio.

paradigms and others can be considered difficult challenges that should be handled in the routing protocol design.

3.1.4 Vehicular Ad hoc Networks

A **V**ehicular **A**d-**H**oc **N**etwork (VANET) is the newest paradigm of the wireless multi-hop networks. It emerged from MANETs with the mobile nodes being the vehicles on the roads. Vehicles communicate using a wireless communication in a multi-hop fashion for disseminating information between each other. These connected vehicles are known as *intelligent vehicles* and are equipped with a wireless communication module and sensors that monitor the interior and exterior surroundings and provide assistance/alerts to the driver via an on-board unit (OBU) [12].

Many standards are introduced for VANETs wireless communication with the most dominant is the Wireless Access for Vehicular Environment (WAVE) standard. WAVE is an amendment of the IEEE 802.11 standard for WLAN and it is standardized to be known as IEEE 802.11p [13].

Vehicles communicate together and with the Road Side Units (RSUs) for relaying and sharing messages and information that will support many ITS application domains such as: safety applications (e.g. safety warnings broadcasting), traffic management applications, road conditions monitoring applications, infotainment applications (e.g. Internet access), advanced driver assistance services (ADAS) applications (e.g. automatic toll collection, remote diagnostics), to name a few.

Four communication patterns are available in VANETs communications: 1) beaconing; 1-hop broadcasting for positions and velocity information, 2) geocasting; sending information to an area of interest, 3) unicasting; sending information to a specific destination, and 4) information dissemination; flooding the surrounding area with information [14]. Figure 3 illustrates these communication patterns.

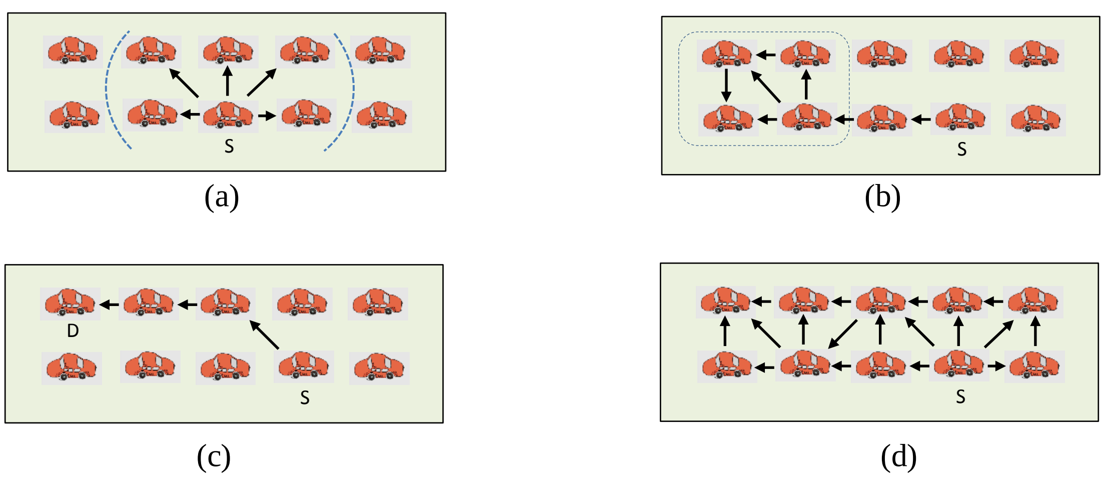

Figure 3 VANETs communication patterns: (a) Beaconing, (b) Geocasting, (c) Unicasting, and (d) Information dissemination.

Among these communication patterns, geocasting, unicasting, and the information dissemination patterns are based on multi-hopping for delivering information. Both geocasting and unicasting require establishing a routing path between the source and the destination (which may be a specific area or node). Information dissemination may not need finding a definitive route but needs some routing functionalities for handling data redundancy and broadcast storms.

There were many trials for using MANETs routing protocols with VANETs, based on the idea that VANETs is a special type of MANETs. These trials did not achieve the expected performance as the VANETs environment showed that it incurs some unique challenges and features that entail the development of a set of new routing protocols or the adaptations of some current MANETs protocols to meet the vehicular environment needs. Some of these distinguishing challenges and features are:

a) Highly Dynamic Topology

Since vehicles are moving at high speeds (especially on highways), the topology in VANETs is subject to frequent changes. Routing protocols should provide mechanisms for maintaining the followed routes and handling link changes.

b) Intermittent Connectivity

It can be a common case in VANETs that a vehicle will not find a neighbor in its vicinity to forward its data to and it will have to keep the data till it comes into contact with another vehicle. This will be the case in sparse environments. Even in dense environments, traffic lights and stop signs may lead to some network partitions. Routing protocols should provide mechanisms for handling this intermittent connectivity. The most common mechanisms are the Store-Carry-Forward mechanism for the delay-tolerant networks and either the use of RSUs for relaying messages, or depending on finding an alternative path using a recovery mechanism in the delay-sensitive networks.

c) Restricted Mobility Patterns

Vehicles mobility patterns are restricted by roads topology and speed limits. This may be considered advantageous because these restricted patterns can help in predicting future events (e.g. traffic conditions per road and vehicles positions). This feature will help the routing protocols to take more informed decisions [15].

d) Sufficient Resources

Vehicles have several advantages over other types of mobile nodes: abundant power, processing, and storage resources; these will provide more flexibility for routing protocols design. VANETs routing protocols can relax the need for energy-efficient routing mechanisms. In addition, having sufficient processing and storage resources, VANETs routing protocols do not have to be compact in size and complexity.

e) Delay Constraints

As the most common applications supported by VANETs are the safety ones, this kind of applications impose hard delay constraints. Routing protocols should ensure continuous connectivity for such applications to avoid any incurred delays for disconnections and expedite the connection setup times to keep the transmission delay as low as possible.

f) Availability of Information Providers

The vehicle’s sensors readings can be utilized in the routing protocols to enhance their functionalities. For example, GPS position information and the vehicle’s speed obtained from the speedometer can be used to assist in designing efficient location-based routing protocols. Unlike the other types of networks where position and velocity information require adding special components to the nodes, most vehicles already have these reading providers built-in. In addition, with the availability of the on-board unit that can have access to navigation software and road maps, these sources of information can help routing protocols to make better informed decisions regarding the optimum paths.

All these distinguishing challenges and features should be considered in designing a routing protocol for VANETs to be as efficient as possible and to meet the requirements and needs of the vehicular environment; the most important design considerations are handling the highly dynamic topology and intermittent connectivity to maintain connectivity among vehicles.

3.1.5 Discussion

Many factors can be used to profile the four multi-hop network paradigms. The most prominent factors are outlined in Table 1 and discussed in details in the following paragraphs.

- ***Network size*** refers to the number of nodes that typically constitute the network. Network size will affect the scalability of routing techniques and should be a primary design consideration.
- ***Terrain scope*** which is open for VANETs, while in the case of MANETs and WMNs the terrain is limited due to the deployment requirements. WSNs scope will highly depend on the application requirements; in applications such as animal monitoring, the scope will typically be large, while in industrial deployments the scope is limited to a building.
- ***Mobility degree*** and ***topology change*** are highly correlated, since a high degree of mobility (as is the case with MANETs and VANETs) implies a network that is frequently changing.
- ***Type of traffic*** refers to the type of data sent over the networks in that paradigm. It is highly related to the objectives and the kind of applications that network paradigm supports.
- The degree of required ***connectivity*** in MANETs is medium since the communication tasks do not require all of the nodes to be connected at all times. This is also the case in WSNs where the large number of nodes allows for reliable execution of the deployment task without the need for all nodes to be connected at all times. Since the main goal of WMNs is to provide wireless broadband access, it is imperative that a high degree of connectivity be maintained among mesh routers. In VANETs, when it comes to safety applications that drive their deployment, vehicles must be highly connected.
- ***QoS*** is a critical factor for the WMN for providing broadband services and it can be considered tolerable for the other network paradigms.
- When it comes to ***energy constraints,*** WSNs suffer the most due to the limited battery power available to a sensor node.
- In terms of the ***availability of computational resources,*** MANETs' nodes range from smartphones to PDAs and laptops, so the resources availability can range from medium for the smaller devices to high for laptops. Nodes in WMNs and VANETs can afford to do sophisticated computations while WSNs nodes have very limited resources and should do minimal functionality.
- ***Location dependency*** refers to the need for network nodes to be location-aware for the proper execution of the functionalities required by the applications that these networks are deployed to do. VANETs are the most dependent on location information as the position-based protocols are the best candidates for VANETs.
- Different ***addressing schemes*** are utilized by the four networks; MANETs and WMNs follow the classic IP-based addressing scheme, while VANETs deploy a mix of unique vehicle identifiers together with the specific location of a vehicle node at a given time. WSNs use data-centric addressing which is based on attribute-value pairs for both the interests and data.

All of the above factors affect the routing function, either directly or indirectly, and should be considered as a part of the design considerations of the routing techniques deployed for each of the networks for its proper operation.

Table 1 compares the four wireless multi-hop network paradigms in terms of these factors.

Table 1 Comparison of Wireless Multi-hop Networks Characteristics.

	MANETs	WSNs	WMNs	VANETs
Network size	Medium	Large	Medium	Large
Terrain scope	Limited	Application-specific	Limited	open
Mobility degree	High	Limited	Static	Very high (constrained)
Topology change	Dynamic	Quasi-stationary	Stationary	Highly dynamic
Type of traffic	Simple	Low-rate	Broadband	Safety+infotainment
Connectivity	Medium	Medium	High	High for safety applications
QoS level	Tolerable	Tolerable	Critical	Tolerable
Energy constraints	Low to Medium	High	Low	Low
Available computational resources	Medium to High	Low	High	High
Location dependency	Low	Application-specific	Low	High
Addressing scheme	IP-based	Data-centric	IP-based	Location-based

3.2 Classification and Directions

In this sub-section, we will shed light on the popular classification for the routing protocols of each network paradigm.

3.2.1 Mobile Ad-Hoc Networks

The most popular classification of routing protocols in MANETs is the classification according to how the route is being discovered. For discovering a route or path, the routing protocol can follow the *proactive*, *reactive* or *hybrid* techniques, as shown in Figure 4 .

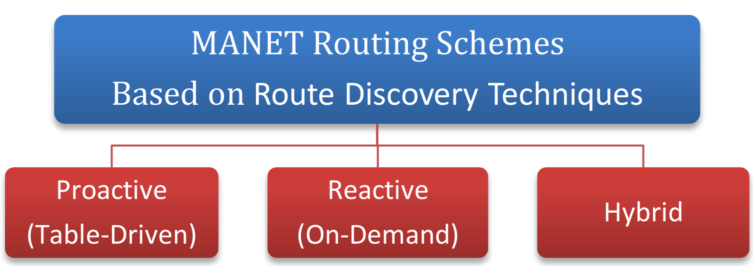

Figure 4 Classification of MANET Routing Protocols.

3.2.2 Wireless Sensor Networks

As the hierarchical and position-based routing schemes are common in WSNs to enhance scalability and improve energy efficiency, it is preferable to classify routing protocols according to network structure as illustrated in Figure 5. The routing protocols can be classified as *position-based* or *topology-based* protocols.

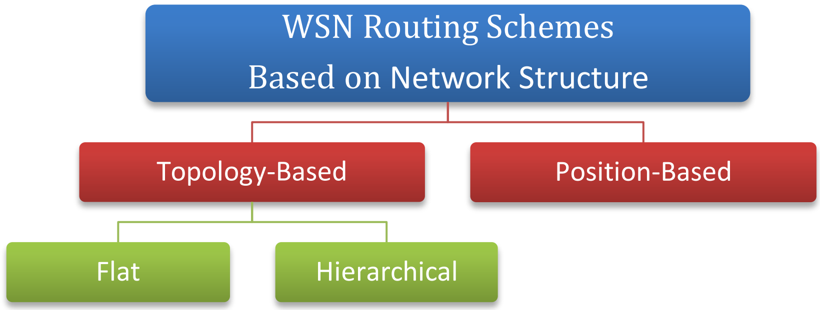

Figure 5 Classification of WSN Routing Protocols.

- **Topology-Based Routing**

Topology-based routing depends on the use of information about the links and edges connecting the nodes in establishing routes. It can be further classified into *flat* and *hierarchical* routing.

- Flat Routing

  In the flat networks, all nodes are in the same level and they all play the same role and collaborate together to perform the sensing task [16].

- Hierarchical Routing

  In the hierarchical protocols, nodes are divided into structuring layers (e.g. clusters, trees.) with the nodes in a layer collecting data from a lower layer, aggregating this data to reduce the number of transmissions and then sending the aggregated data to an upper layer[5]. In this type of network, nodes are usually assigned different roles depending on their layer of operation and they may have different capabilities based on their role in the network.

- **Position-Based Routing**

The position-based routing protocols depend on the use of position information for forwarding packets. In this type of network, nodes are addressed by their geographical location and it is assumed that the nodes are aware of their locations by using GPS or localization techniques. To determine the current position of the intended destination, the source node uses a location service to get the position and include it in the packet's destination address. Mobile nodes register their current position with the service [17].

3.2.3 Wireless Mesh Networks

Routing protocols in WMN can be classified with different taxonomies. For example, protocols can be classified based on: route discovery (proactive, reactive, or hybrid), network variations (static or

[5] It may be the sink or another layer for further aggregation.

dynamic), protocol management (distributed, centralized, or hybrid), etc. Since the main goal of a WMN routing protocol is providing guaranteed QoS and satisfying the network performance objectives, one of the best taxonomies for the WMN routing protocols is based on performance optimization objectives that is presented in [18] and shown in Figure 6. According to this taxonomy, WMN routing protocols can be classified into either *hop-count based* protocols, *link-level QoS* protocols – which can be further classified into *link quality*, *interference*, and *load balancing* protocols-, *end-to-end QoS* protocols, *reliability-aware* protocols, or *scalable routing based* protocols.

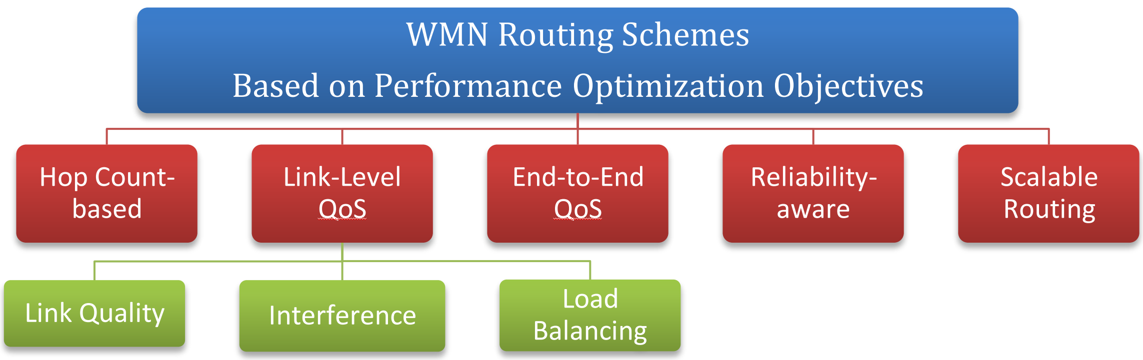

Figure 6 Classification of WMN Routing Protocols.

- **Hop-Count Based Routing**

Protocols under this category utilize the hop-count metric for the optimum route selection. These protocols have the advantage of simplicity but they usually fail to achieve the desired QoS level.

- **Link-Level QoS Routing**

These protocols measure quality of a route in a hop-by-hop basis at the link level. Their objective is minimizing the accumulative or bottlenecked link-level effects by considering the status of each link along the path. For measuring link quality, these protocols depend on the use of parameters such as packet loss rate, retransmission count, transmission time. This type of routing optimizes the performance objectives related to the link quality, interference, or load balancing [18].

- **End-to-End QoS Routing**

These protocols consider the route QoS in an end-to-end basis. Such protocols achieve better performance than the link-level ones. They depend on measuring end-to-end parameters such as delay, bandwidth, and packet delivery rate.

- **Reliability-Aware Routing**

The objective of this category of protocols is assuring reliability of routing by applying different approaches. The most common approach is utilizing multipath routing. Multiple paths will be available to provide fault tolerance for the routing process and/or traffic distribution over the entire network.

- **Scalable Routing**

Protocols under this category are designed for large scale WMNs. Scalability of a routing protocol can be supported by following different routing approaches such as the hierarchical and geographic approaches [18].

3.2.4 Vehicular Ad hoc Networks

VANETs routing protocols can be either MANETs protocols that are found/amended to be suitable for the vehicular environment and characteristics, or specifically-designed protocols that are designed with the VANETs challenges and features considered. Based on this view, VANETs routing protocols can be classified either to be *topology-based* or *position-based* protocols. This classification is illustrated in Figure 7.

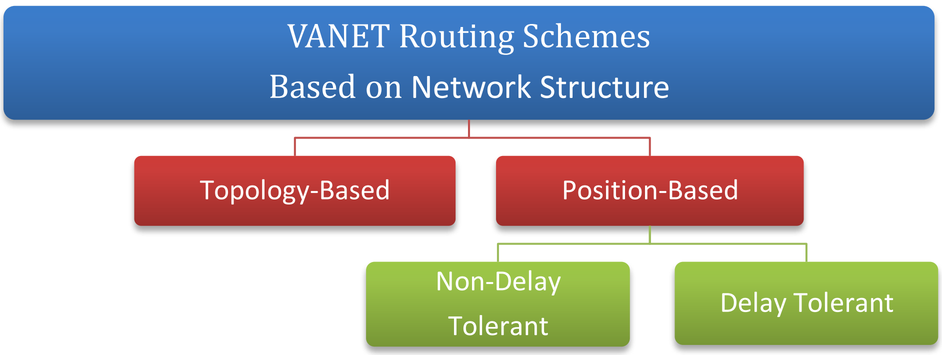

Figure 7 Classification of VANET Routing Protocols.

The *topology-based* protocols are the MANETs protocols that are suggested to be suitable for use with VANETs. As they are not designed specifically with the VANETs requirements and features in mind, the topology-based routing protocols did not prove to be efficient compared to position-based protocols.

The *position-based* routing protocols proved to be the best candidates for the VANETs routing functions. Some of these protocols are inherited from some MANETs ones and others are newly-designed. With remarkable performance improvements on the topology-based category, the category of position-based routing is the commonly-used and studied one. Most of the protocols available in the literature and those that are currently being proposed are based on this routing scheme.

The position-based protocols can be further classified into delay tolerant protocols and non-delay tolerant protocols.

- **Delay Tolerant Protocols**

These are the protocols designed for applications that can have some delays in delivering packets without affecting performance requirements. The packets can be kept in buffers at the nodes and delivered in subsequent time [19] [20].

- **Non Delay-Tolerant Protocols**

These are the protocols designed for the delay-sensitive applications. These protocols should deliver the packets in time; otherwise, the objectives of the applications will fail [71].

3.2.5 Discussion

In this section, we discussed the most common classification and taxonomy for each paradigm of the wireless multi-hop networks.

The basic classification is the one based on the route discovery and this is the one we used for classifying the routing protocols of MANETs.

As proactive routing is not common in WSNs due to its control packets overhead, the WSN routing protocols are commonly classified according to a different taxonomy. As the hierarchical and position-based protocols are common in WSNs due to their scalability features, the best classification for the routing protocols of WSNs is based on the network structure.

As the main objectives of WMNs is achieving a satisfactory QoS level and meeting desired performance goals, the best taxonomy for the WMN routing protocols is the one based on the performance optimization objectives. A WMN routing protocol is classified according to the performance objective that it is working on to achieve.

Lastly, as VANETs utilize the position-based protocols heavily because they are the most suitable ones for their addressing scheme - location-based - and because they also inherit some topology-based protocols from MANETs, the best taxonomy for the VANET routing protocols is the one based on the network structure.

3.3 Core Components and Functionalities

Core components are inherited in all routing protocols for all wireless multi-hop networks. In addition, routing protocols for each network paradigm may have auxiliary components that are added to meet the requirements and challenges of this network paradigm. Such components are crucial in some network paradigms to provide the needed efficiency; therefore, these components will be also considered core ones for that specific network paradigm.

In this section, we will discuss the core components of each wireless multi-hop network paradigm showing which auxiliary components will be activated and considered as core for that network paradigm. We will also explore different functionalities deployed by the routing protocols for handling the operation of each of these components and some representative routing protocols that include these functionalities.

3.3.1 Mobile Ad-Hoc Networks

The most critical challenge in designing a routing protocol for MANETs is handling nodes mobility to maintain network connectivity. As the nodes are free to move, the network topology incurs frequent changes in the links connecting nodes and the neighborhood of each node, thus, links are usually prone to failures. To maintain connectivity and achieve a satisfactory degree of reliability in MANETs, the route maintenance component is a crucial part of any MANET routing protocol. In addition to the three core components – route discovery, route selection, and route representation and data forwarding – route maintenance is activated from the set of auxiliary components and is considered one of the core components of MANETs routing.

a) Route Discovery

Route discovery in MANETs involves different functionalities depending on the category of the protocol; proactive, reactive or hybrid. Also, under each category, there are various approaches for performing the route discovery stage.

Proactive protocols may differ in:

- *the kind of topology information exchanged among the nodes,*

  Some protocols are based on distance vectors exchange (e.g. Destination Sequence Distance Vector (DSDV) [21], Wireless Routing Protocol (WRP) [22]), and others depend on the exchange of link state packets (e.g. Fisheye State Routing (FSR) [23], Optimized Link State Routing protocol (OLSR) [24]).

- *the contents of the routing information,*

  For example, the DSDV protocol shares information about the destinations, the number of hops to reach that destination, and the last sequence number seen from that destination to distinguish the stale routes from the fresh ones in order to avoid routing loops. The Distance Routing Effect Algorithm for Mobility (DREAM) [25] exploits the location and speed information of the nodes for routing packets and it depends on disseminating the network with location information by sending location updates. Being a cluster-based protocol, nodes in the Clusterhead Gateway Switch Routing (CGSR) protocol [26] periodically broadcast a cluster member table which maps each node to its respective cluster-head.

- *to which nodes the topology information is sent,*

  Some protocols send topology information only to their direct neighbors (e.g. DSDV, WRP, FSR, CGSR) and others flood the network with this information (e.g. OLSR).

- *how frequent this information is sent,*

  Sending the routing information is done periodically or upon the occurrence of topology change; whichever comes first. Some protocols do not use a fixed update period. For example, the FSR protocol uses different routing update periods for the different entries in the routing table to reduce the size of the update messages. The entries corresponding to the nearby nodes are sent with higher frequencies than those which are for the far nodes. Another example is the DREAM protocol where the frequency of the updates is a function in the node mobility.

- *how flooding of topology information is handled,*

  Flooding is usually performed by disseminating packets to the whole network. This kind of communication is known as *blind flooding* and it incurs traffic overhead and may lead to congestion in the network. Some protocols try to reduce the flooding overhead by utilizing techniques to limit the range of transmission or to limit the number of forwarding nodes. For example, the OLSR protocol depends on the use of Multi-Point Relays (MPRs) to distribute the routing information through the network. The MPR set of each node is the minimum number of direct neighbors that cover all the two-hop neighbors of that node. By using this technique, the number of nodes involved in disseminating the routing information is reduced; hence, the flooding overhead is mitigated. Another example is the Core-Extraction Distributed Ad Hoc Routing (CEDAR) protocol [27] where a subset of the nodes in the network are identified as the “core” nodes. These core nodes are determined using a distributed algorithm which ensures that each node has at least one adjacent core node. The link state information is propagated only through the core nodes.

- *the number of routing tables used by each protocol*

  Protocols may utilize different number of tables to support their operation. For example, DSDV uses only one routing table where it stores the cost to each possible destination in the network along with the next hop to this destination and a sequence number that is assigned by the destination to specify how fresh the route is. Unlike DSDV, WRP maintains four different tables; a routing table, a distance table, a link-cost table, and a message retransmission list.

For route discovery, the ***reactive*** protocols employ different approaches for sending the route request (RREQ) packets through the network:

- Some protocols flood the whole network with the RREQ packets (e.g. the Dynamic Source Routing (DSR) protocol [7]). In DSR, when a node receives a RREQ, if it is the intended destination, it returns a route reply (RREP) packet carrying the whole accumulated route that it gets from the received RREQ. If it is an intermediate node and has a route for that destination stored in its cache, it concatenates the part of the route it has to the part in the received RREQ then sends the whole route in a RREP back to the source. Otherwise, the intermediate node forwards this RREQ to its neigbors after appending its address to the route list in the request. Usually, The RREP follows the reverse route back to the source. This is only possible if symmetric links are available. Otherwise, to send the RREP back to the source, the responding node initiates a route discovery process and piggybacks the RREP to the new RREQ.
- Other protocols try to reduce the flooding overhead by limiting the number of forwarding nodes or the dissemination area. For example, the Ad Hoc On-Demand Distance Vector (AODV) routing protocol [28] employs the ring-search technique to handle cases where the destination is quite near the source. In such cases, flooding RREQ packets through the whole network is wasteful. To handle that, the idea of the ring search scheme is based on searching larger areas successively. First, RREQ is disseminated in the area around the source. If the destination is not found, the searching area is widened and so on till the destination is found. To control the area of searching, the TTL field of the RREQ packet is assigned to 1 first then increased with widening the area of interest in which the source is centred.
- Other protocols depend on exploiting the location and speed information to limit the RREQs flooding to a certain zone. An example is the Location Aided Routing (LAR) protocol [29] in which this zone is known as the request zone. In LAR, for route discovery, the source first estimates the expected zone where the destination is expected to be within. This zone is calculated based on the last known position for the destination, the last time to hear from that destination, the current time, and the speed of that destination. The flooding of RREQs is limited to the request zone which includes the expected zone and the location of the source node. Nodes out of the request zone discard the RREQ packets.

For the **hybrid** route discovery, most protocols depend on deploying a proactive technique for reaching the local nodes and reactive one for reaching remote nodes:

- For example, the Zone Routing Protocol (ZRP) [30] divides the network into zones. The zone of a node is the nodes that are up to h hops from that node. ZRP employs two different routing approaches for the intra-zone and the inter-zone packets. Inside a routing zone, a proactive IntrA-zone Routing Protocol (IARP) is used. For communications with nodes in different zones, a reactive IntEr-zone Routing Protocol (IERP) is used. Both the IARP and the IERP performs route discovery as specified by the used proactive and reactive protocols respectively.
- Another example is the Zone-based Hierarchical Link State (ZHLS) routing protocol [31] which assumes that the nodes know their physical location and divides them into zones based on the geographical information. Each node periodically broadcasts information about its neighbors to the nodes in the same zone and this information is stored in an intra-zone routing table. When a node

has a packet to send, it checks first its intra-zone table. If the destination is out of its zone, the source node sends a location request to all other zones via gateways. When a gateway of the zone where the destination is receives this location request, it replies to the source with a location response containing the zone ID of the destination.

b) Route Selection

Most protocols depend on the use of only one selection metric that is determined based on the application needs. Some protocols may utilize multiple selection metrics that can be combined by a means of optimization function.

In the **proactive** protocols, route selection is done implicitly with the exchange of the up-to-date route information. When a node receives the topology information packet, either distance vector or link state, it updates the routes stored in its routing table according to the received updates.

The process of route selection in the **reactive** protocols is an explicit process that may be handled using one of three approaches; source-based, destination-based, or intermediate-based selection:

- An example of a protocol utilizing **source-based** route selection is the DSR protocol. In DSR, the destination replies to all RREQs it gets then it is the responsibility of the source, after getting the RREP packets, to pick one path for forwarding the data through.
- The Load-Balanced Ad-hoc Routing (LBAR) protocol [32] utilizes **destination-based** route selection technique. It defines a new metric for route selection known as the degree of nodal activity which is defined as the number of active paths through a node. Also, it defines Traffic Interference as the sum of neighboring activity of the current node. During its route discovery phase, each intermediate node along a potential path to the destination calculates its nodal activity and traffic interference and these values are added to the path cost got from their preceding nodes. When the destination receives the routing information, it chooses the path with the minimum cost; least activity. Another protocol that utilizes destination-based selection is the Zone-Based Routing (ZBR) protocol [33] in which the destination picks the path with the highest stability. It depends on dividing the network area into non-overlapping square zones and determines the path stability based on the mobility factor of the nodes along the path.
- As an example of **intermediate-based** route selection protocol, the Greedy Perimeter Stateless Routing (GPSR) protocol [34] utilizes hop-by-hop route selection. It is based on greedy routing in which the neighboring node closest to the destination is chosen to be the next forwarding node.

For the **hybrid** protocols, route selection is a combination of the route selection techniques utilized by their underlying proactive and reactive parts.

c) Route Representation and Data Forwarding

Route representation and data forwarding can be handled using two different techniques; exact route and route guidance. The exact route technique can be further performed using either routing tables or source routing.

- An example of the protocols that deploy the source routing approach is the DSR protocol. DSR is one of the most well-known protocols of MANETs and many other protocols inherited the idea of source routing from it. Another example is the Cluster Based Routing Protocol (CBRP) [35] which exhibits the idea of the DSR routing protocol. Unlike DSR which is a flat protocol, CBRP deploys source routing in a clustering-based fashion; only the clusterheads addresses are recorded in the accumulated address. The clusterheads can communicate via the gateway nodes which are the nodes in the overlapping area between the clusters. The information about the adjacent clusters and the gateways to these clusters is stored in a cluster adjacency table.

- There are many protocols that depend on the use of routing tables for route representation and data forwarding. Examples are all the proactive routing protocols (e.g. DSDV, WRP, FSR, OLSR, CGSR). Some reactive protocols also depend on the use of routing tables for storing routes and next hops for the route reply and data packets and use these stored information to forward these packets. Example is the AODV protocol in which a node receiving a RREQ records the address of the node from which it received the first RREQ in its route cache to use it in returning the route reply back to the source. This is how the reverse path is created. Also, while returning the RREP back to the source, all nodes along the path keep an entry for the node from which it received the RREP and this is how the forward path is created.
- The GPSR protocol is an example of the protocols that utilize route guidance techniques. GPSR is a position-based protocol that adopts greedy packet forwarding to send a packet to a specific destination.

d) Route Maintenance

Route maintenance is handled differently according to the category of the routing protocol; being proactive, reactive, or hybrid. In the **proactive** protocols, route maintenance is done implicitly with the exchange of routing updates. Having up-to-date routing information at each node helps in handling any changes in the network topology.

In the **reactive** protocols, discovered routes are usually stored in a route cache in the nodes that involved in a transmission on those routes. These routes should be refreshed for the nodes to ensure their validity. Also, they should be invalidated when expired in order not to use them in subsequent transmissions. Also, failures of these routes should be handled either locally or by the source nodes if these routes are still needed for further transmissions. The reactive protocols use various approaches to support all the processes related to the route maintenance operation. For example:

- In DSR, each node should make sure that the packet is received by its next hop by means of acknowledgment (either acknowledgment provided by the link layer protocol or by passive acknowledgment). Otherwise, the node should retransmit the packet (up to a certain limit). When the limit of retransmission is reached, the sending node should look for an alternative path to the destination in its cache. If there is no other alternative, the sending node sends a Route Error packet to the source with information about the broken link. The source should remove the broken link from its cache and start the route discovery process again.
- In AODV, to maintain local connectivity, if a node has not sent any packets to its active neighbors for a predefined period, the node broadcasts a Hello message to inform its neighbors that it is still there and alive. If any node along a route has moved, this can be detected by its predecessor that will generate a link failure notification message and sends this message to the active neighbors of this route. These neighbors send this message to their active neighbors and so on till it reaches the source which can reinitiate the route discovery process if it still needs to send data to that destination.
- The CBRP protocol deploys a Local Repair mechanism. With the Local Repair, if a node detects that its next hop is unreachable, it tries to salvage the packet. It checks the source information in the

packet to get the hop after the next[6] then it checks its neighbor table and looks for a neighbor node that can reach the next hop or the hop after the next. If any of these two hops is reachable by one of its neighbors, the packet is forwarded through the new route.

- The Temporally Ordered Routing Algorithm (TORA) protocol [36] depends in its operation on creating a Directional Acyclical Graph (DAG) from the source to the destination. When a node loses its downstream link, it generates a new reference level and broadcasts the reference to its neighbors. TORA also involves a Route Erasure mechanism for retiring the invalid routes. The erase operation floods CLR packets through the network and erase invalid routes [37].

As the **hybrid** protocols are a combination of both reactive and proactive protocols, route maintenance in the hybrid protocols is also a combination of the route maintenance techniques supported by the utilized proactive and reactive protocols.

3.3.2 Wireless Sensor Networks

The most critical design challenge for WSNs is the energy efficiency. Energy conservation techniques should be included in any WSN routing protocol to be suitable for the characteristics of the WSN, to provide efficient operation and routing functions, and to prolong the network lifetime to be operational for many years without intervention from the network designers who, in many cases, will not be able or willing to recharge the network nodes[7]. Therefore, in addition to the three core components, the energy efficiency component will be activated and considered a core one.

The WSN has its own unique data-centric addressing scheme based on the attribute-based addressing. In WSNs, the interest is on the data itself and the area where it is sensed not on which nodes are reporting this data. Therefore, establishing routes is not based on finding a path to a specific destination with a specific address. There is a sole destination which is the BS or the dedicated data collector that collects the reported data for further analysis. The location of the BS is known and, in most cases, it is unchangeable throughout the whole operation of the network. The focus is not on discovering and selecting an optimum route; the focus is on reporting and forwarding the data to the BS. Route discovery and selection is done in parallel with the data forwarding stage. Since the operation of these stages is combined together, we propose merging the three core components - route discovery, route selection, and route representation and data forwarding - into one core component which we call Route Establishment and Data Forwarding. With the introduction of the new, mixing routing component, the core components of the WSN routing protocol are the Route Establishment and Data Forwarding component and the Energy Efficiency component.

a) Route Establishment and Data Forwarding

Communication in WSNs can be either 1) data-based with the nodes commencing the communication with reporting or advertising the data they have either in a time or event-driven basis, or 2) query-based with the BS issuing data interests and disseminating them through the network asking for specific sensing tasks. Based on these communication patterns, we classify the route establishment and data forwarding techniques into either **source-initiated** or **sink-initiated** techniques:

[6] CBRP employs source routing, so, the whole path is stored in the data packet.

[7] For example, it may be infeasible or impossible to change the batteries for the nodes deployed in harsh or hostile environments.

1) Source-Initiated

Many protocols depend on the source-initiated techniques and these protocols are typically designed for applications like the data gathering or object tracking applications. Some of these protocols depend on sending their actual data to the data collector without any prior negotiation and others deploy preceding the actual data transmission with a kind of meta-data advertisement for conserving the energy that may be wasted for sending and receiving data that are not in interest to others. What follows are examples of protocols that utilize source-initiated techniques:

- *Actual Data Transmission Based*

- The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol [38] is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs. Nodes in LEACH are partitioned into clusters with each cluster member reporting data periodically to its cluster head (CH). Each CH collects the data from its cluster members, aggregates them, and sends them directly to the BS. The CHs election is a distributed, stochastic, energy-aware process that is run locally at the nodes. Heinzelman et al. also presented a variant, called LEACH-Centralized (LEACH-C), which moves the burden of the CHs election to the BS.
- The Minimum Cost Forwarding Algorithm (MCFA) [39] exploits the fact that the destination is always known; it is the BS. In MCFA, each node maintains the least cost estimate from itself to the sink. The source broadcasts the data to its neighbors. A node receiving a packet will rebroadcast it if the node is on the least cost path between the source and the sink.
- The Power-Efficient Gathering in Sensor Information Systems (PEGASIS) protocol [40] is hierarchical chain-based protocol. The chain in PEGASIS is the set of nodes that are closest to one another and form a path to the BS. Each node sends its data only to its next node in the chain, the nearest one to it. Each chain has a chain leader that collects the data from other nodes in the chain, aggregates them, and sends them directly to the BS.

- *Meta-Data Transmission Based*

- The Sensor Protocol for Information via Negotiation (SPIN) [41] is a family of flat protocols that depends on the idea of data dissemination through the whole network assuming that all nodes are possible BSs. SPIN uses an intelligent data dissemination mechanism to reduce receiving redundant and unnecessary data from sensors monitoring overlapping areas and avoid the implosion problem. It achieves this by using a data negotiation algorithm. Nodes in SPIN form meta-data that represents the actual data but with much less size and is sent in an ADV message. SPIN is a three-stage handshake protocol that includes the use of three messages: ADV, REQ, and DATA that represent the three stages. The family of SPIN protocols can also be suitable for an environment with mobile sensors as data is disseminated through the whole network.
- Another example is a variant of the LEACH protocol called LEACH with negotiation [38] which inherits the main idea of SPIN. In LEACH with negotiation, cluster members precede the actual data transmission with a negotiation phase with its CH to ensure that only new data is transferred to the CH to avoid data redundancy.

2) Sink-Initiated

Sink-initiated protocols are based on the query/interest-based communication pattern. These protocols involve different functionalities based on how queries/interests are sent. Queries can either be flooded through the whole network or sent to an area of interest based on location-aware mechanisms. In the following, we will shed light on some protocols and functionalities that utilize the sink-initiated mechanisms:

- *Flooding Based*

- The Directed Diffusion (DD) protocol [42] is one of the most popular WSN routing protocols. It is a flat, data-centric protocol in which the interest is named as an attribute-value pair that describes a sensing task. The response is described with a similar attribute-value naming. It starts with the sink flooding exploratory interests through the whole network. When a node receives an interest, it sets up a gradient toward the neigbhor from which it received the interest. So, the gradients determine the path back to the originator of the interest. Sensors that hold data matching the interest send the requested data along the gradients. In the exploratory phase, the sensed data is reported with a low rate to the sink. The exploratory phase is followed by a reinforcement phase to get the data with higher rate for more accurate event detection through specific nodes along a specific path. Choosing the neighbor that to be reinforced can be based on many criteria. The simplest way is to reinforce the neighbor from which the first response for the interest is received. This way, the reinforced path will be the path with the lowest delay.
- The Rumor Routing protocol [43] is a variation of the DD protocol. Its key idea is to limit flooding to the nodes that have observed events rather than to the whole network. It uses agents packets and events table to minimize the interest flooding overhead of DD.
- The Gradient-Based Routing (GBR) protocol [44] is another variant of DD. The key idea of GBR is memorizing the number of hops when the interest is diffused. Each node calculates its height which is the minimum number of hops to reach the BS. The difference between the node height and that of its neighbor is considered the gradient of the link. The link with the largest gradient is selected.
- The Reliable Energy Aware Routing (REAR) protocol [45] is based on flooding interests but instead of discovering only a single path between a source and the sink, REAR discovers an additional backup path to the same source. In discovering the backup path, only the nodes that are not involved in the service path will broadcast the backup path request to maintain two completely disjoint paths. REAR also utilizes a path reservation mechanism in which every intermediate node on the path will mark part of its energy as reserved for this path.
- The COUGAR protocol [46] separates the query processing task from the network layer and adds another layer, the query layer, between the network and the application layers. It represents the network as a huge database system with the BS being responsible for generating the query plan, defining the query flow and its in-network computation and forwarding it to the relevant nodes [47].

- *Location-Aware Based*

- An example is the Geographical and Energy Aware Routing (GEAR) protocol [48] which is considered an improvement of the DD protocol. It exploits the fact that the interests are usually formed for a target region and they carry geographical information about it. It uses this geographical information to direct the interests to the target region without flooding. It assumes that each node has information about the location and current energy level of itself and its own direct neighbors which are exchanged by the use of periodic Hello Messages. For forwarding a packet, a node computes a cost for each of the neighbors that are closer to the target region. This cost is calculated based on the residual energy of the neighbor and its distance to the centroid of the target region. The node picks the neighbor with the smallest cost to forward the data to. Once the packet gets into the target region, it is disseminated within the region using either restricted flooding or recursive geographic forwarding[8].

b) Route Energy Efficiency

There are many techniques for achieving energy efficiency and reducing energy consumption in WSNs. The following are some of the common techniques utilized by protocols in the literature. One protocol may utilize one/many of these techniques:

1) Use of Meta-Data

- The deployment of the meta-data approach proved to provide great savings in energy efficiency. For example, the SPIN family of protocols are able to transmit up to 60% more data for a given amount of energy than conventional protocols [41].

2) Data Aggregation

- In SPIN, a receiver may perform data aggregation for the received and its own data, if it has any, before advertising the data.
- The DD protocol allows data and interest aggregation. Two interests with completely overlapping attributes can be represented with a single interest entry.
- As a variant of DD, the GBR protocol also utilizes data aggregation.
- In LEACH, each CH aggregates the data received from its cluster members before sending them to the BS.
- Another example is the COUGAR protocol in which sensor nodes select a leader node to perform data aggregation and forward it to the BS.
- In PEGASIS, the chain leader aggregates the data of the other nodes in the chain and sends them to the BS.

3) Use of Resource Manager

- One of the SPIN family of protocols, SPIN-2 (or SPIN-EC), includes a resource manager that monitors the energy consumption of the node and adapts its operation according to its available energy.
- In REAR, a resource manager at each node keeps track of the node energy and suppresses the path-request broadcasting messages to be sent by an energy-weak node.

4) Putting Nodes into Sleep Mode

- In DD, to save power, sensors are kept off until tasked by a reception of an interest.
- Another example is the LEACH protocol which is based on a TDMA scheme. Each member sends its data to the CH in its own time slot and it can go to the sleep mode in the others' slots to conserve its energy.

---

[8] The recursive geographic forwarding divides the target region into four sub-regions and a copy of the packet is sent to each sub-region. The splitting and forwarding procedure is repeated till the sub-region has only one node.

5) Load Balancing

- The LEACH protocol adapts dynamic clustering by dividing time into rounds and, at the beginning of each round the roles of CHs are rotated to balance the energy consumption among the nodes.
- The GBR protocol deploys a traffic spreading technique to balance the traffic load among the nodes. New data streams are not passed through nodes that are currently part of the routes of other data streams.
- Another example is the Energy-Aware Routing protocol [49] which is a variant of the DD protocol. Unlike DD which enforces one path to receive data through at higher rates, the Energy-Aware Routing protocol maintains multiple paths at each node, and selecting the path is based on the energy consumption level of each stored path. Having different paths selected at different times balance the load and energy consumption among the nodes in the network.
- In the PEGASIS protocol, the role of chain leader is rotated among nodes in the chain in a round basis to balance the energy consumption among the nodes.

6) Use of Energy-Aware Metrics

- In addition to deploying dynamic clustering, the CH election process in LEACH is based on the nodes' current residual energy.
- The GEAR protocol depends on the use of an energy-aware heuristics that considers the geographical information as well for selecting the next-hop toward the target region.

7) Use of Restricted Flooding

- The GEAR protocol utilizes restricted flooding as one of the options of disseminating packets within the area of interest.

3.3.3 Wireless Mesh Networks

WMNs are comprised of almost stationary nodes. This feature leads to relaxing the mobility and energy constraints. Therefore, WMNs are not in need for auxiliary routing components. The WMN core components are the main three core routing components; route discovery, route selection, and route representation and data forwarding. The WMN QoS requirements and needs can be handled by special metrics and functionalities involved in the route selection component as will be discussed later in this sub-section.

a) Route Discovery

Some protocols are utilizing proactive techniques, others are depending on reactive ones, and some are based on hybrid techniques for route discovery.

1) Proactive-based

- The Light Client Management routing Protocol (LCMP) [50] makes use of two routing tables for maintaining the topology information; a table for maintaining information about the local mesh clients and another table for recording information about the remote clients with the mesh routers associated to them.

As WMNs are mainly used to cover huge areas, the number of mesh routers and clients may be high to be maintained at each node in the network. So, proactive routing is not preferred to use in WMNs as it will cause storage overhead and bandwidth wasting.

2) Reactive-based

- The Link Quality Source Routing (LQSR) Protocol [51] inherits all the functionalities of the DSR protocol including the ones for route discovery (RREQs and RREPs). It only differs in how a route is selected as it supports link quality metrics. The Multi-Radio LQSR (MR-LQSR) protocol [52] works similar to LQSR with supporting multi radio operations.
- Many protocols (examples mentioned later in this section) are based on the reactive hop-by-hop routing approach; no discovery for the full route should be completely done a priori. The next hop is discovered and determined on the fly based on the links status.

3) Hybrid

- The Orthogonal Rendezvous Routing (ORR) Protocol [53] is designed for networks that can have directional communications for their nodes. In ORR, each node can determine the position of its neighbors relative to its North. The source sends route discovery packets and the destination sends route dissemination packets in orthogonal directions and a rendezvous point is located in the intersection of these transmissions. The remainder of the discovery process is handled in a reactive way between the source and the rendezvous point and proactively for the remaining part to the destination.
- The AODV-Spanning Tree (AODV-ST) Protocol [54] inherits the AODV functionalities for the intra-mesh traffic and a spanning tree for communications to/from gateways. It is designed for the multi-radio WMNs.

Also, WMN routing protocols can be either centralized or distributed protocols in terms of how route discovery is handled. Most of the protocols available in the literature are distributed. A few are based on centralized techniques. For example, the Integrated Routing and MAC scheduling Algorithm (IRMA) [55] is a cross-layer, centralized, interference-based MAC-Routing protocol with TDMA access mechanism. In IRMA, nodes and topology information is exchanged in a global control plane on a dedicated channel or dedicated time slot [18].

b) Route Selection

Route selection is where WMNs are distinguished from the other wireless multi-hop networks. It is considered the most important component in WMN routing. Depending on how the route is selected, this will affect how the protocol and the network as a whole will satisfy the performance requirements and QoS guarantees.

As the WMN has its own objectives that are represented in satisfying a reasonable level of QoS and load balancing, many unique routing selection metrics are introduced for use in WMNs. They are mostly related to the links quality, interference (both intra-flow and inter-flow), reliability, and many other criteria that are indicators of the path quality and suitability for providing satisfactory QoS.

In Table 2, we illustrate the common route selection metrics introduced and used by the WMN routing protocols available in the literature [18] [56].

Table 2 WMN routing metrics.

Metric	Measures & Selection	Sample Protocol
Hop Count	- Measure number of hops from the source to the destination - Selection of the path with the minimum number of hops	LCMP
ETX (Expected Transmission Count)	- The expected number of transmissions to successfully deliver a packet over a link. - To compute ETX, each node periodically broadcasts probes containing the number of received probes from each neighbor. - Selection of the path with the least sum of ETXs of the links along the path	ExOR
ETT (Expected Transmission Time)	- The expected time to successfully deliver a packet over a link. - ETT adjusts ETX by incorporating the throughput into its calculation - Selection of the path with the least sum of ETTs of the links along the path	AODV-ST
WCETT (Weighted Cumulative ETT)	- An extended version of ETT - Limited to multi-radio mode - Takes into account the use of multiple channels - Captures the transmission time on the bottleneck channels - Selection of the path with the least WCETT	MR-LQSR
ENT (Effective Number of Transmissions)	- Built on top of ETX - Considers the mean and variance of the packet loss ratio to project physical-layer variations - Selection of the path with the least	Quality-Aware routing [57]

	ENT	
MIC (Metric of Interference and Channel-Switching)	- Considers both inter-flow and intra-flow interference - Calculates its value based on the ETT metric - Adds the number of interfering nodes to the ETT value to compute inter-flow interference - Computes a channel switching cost to measure intra-flow interference - Selection of the path with the least MIC	Load and Interference Balanced Routing Algorithm (LIBRA) [58]
BLC (Bottleneck Link Capacity)	- Indicates the residual capacity of the bottleneck link of a routing path - Based on the expected busy time (EBT) of transmitting a packet over a link - EBT can be measured based on the packet loss rate and transmission mechanism in the MAC layer - The residual capacity of a link is defined as the ratio between the idle time and EBT - Selection of the path with the largest BLC	Capacity-Aware Routing (CAR) [59]

The most common technique for measuring metrics parameters is sending *probe packets*. Probe packets can be sent either in a unicast or broadcast mode. Generating and sending probe packets can be done either *actively*, *passively*, or in *cooperative* approach. In "*active*" probing, special probe control packets are generated and exchanged for this purpose. In "*passive*" probing, data packets can be utilized for the probing purposes too, so, no extra overhead is needed. In "*cooperative*" probing, a node overhears data packets transmitted by its neighbors to estimate the link quality to each neighbor. Active probing is considered the most common measurement technique [60].

c) Route Representation and Data Forwarding

Some protocols are based on exact route representation and others are utilizing some route guidance for data forwarding.

1) Exact Route

- As the LQSR protocol is a variant of the DSR protocol, it makes use of the source routing approach.
- The Multipath Mesh (MMESH) protocol [61] is based also on the source routing approach with allowing the source to have multiple paths for reliability purposes.

2) Route Guidance

- The Extremely Opportunistic Routing (ExOR) protocol [62] follows the self-routing approach; not having an explicit routing path before data transmission starts. In ExOR data packets are buffered and broadcast as batches. Among the nodes that receive this batch, only one node will be selected to forward it and this is what is known as the *opportunistic* routing.
- The Resilient Opportunistic Mesh Routing (ROMER) protocol [63] also follows the opportunistic routing approach. In ROMER, each packet carries a cost that is set by the source node and decremented with each hop according to the WMR cost. Duplicates of the packet may be sent through the network if the packet has enough credit at many forwarders.

Some protocols apply *network coding* for their routing functions to reduce the transmissions and utilize the bandwidth efficiently. In network coding, each transmission carries the information of multiple packets coded all together and decoded at the destination. It can be either applied to packets belonging to the same data flow (*intra-flow network coding*) or packets belonging to different data flows (*inter-flow network coding*) [60]. An example of the intra-flow network coding routing protocols is the MAC-independent Opportunistic Routing & Encoding (MORE) protocol [64] and an example of the inter-flow ones is the Distributed Coding-Aware Routing (DCAR) protocol [65].

3.3.4 Vehicular Ad hoc Networks

The most important challenge for designing a VANET routing protocol is maintaining connectivity while nodes (vehicles) are moving at high speeds causing frequent topology changes. For that reason, route maintenance is required to be included in all VANET routing protocols and the route maintenance component will be activated and considered a core component in VANETs. By the inclusion of the route maintenance component as a core one, the core routing component for VANETs routing protocols are the route discovery, route selection, route representation and data forwarding, and route maintenance components.

Following is a discussion of the common functionalities for each component and some examples of routing protocols that utilize these functionalities. In our discussion, the focus is on the position-based functionalities and protocols as these are the dominating ones in VANETs.

a) Route Discovery

Before discovering a route, the destination location (either location of a specific node or the centroid of an area of interest) needs to be known for the source first. Many location services are available now and they can be accessed easily via the OBU, such as:

- Acquiring the destination position by disseminating query messages. When a destination receives a query message asking for its position, it replies to the source with a response including its current position.

- Use of distributed location services to which the nodes periodically send updates about their positions and velocity vectors. A source can consult these location servers to obtain the current position of a specific node [15].

After obtaining the intended destination position, the process of finding a route to that destination comes next. VANETs routing includes different functionalities for discovering routes. We can consider VANETs protocols in the literature to be all reactive ones. As there are huge numbers of nodes in the network and these nodes connectivity is highly changing, the proactive protocols will not be feasible solutions as there will be a great overhead for recording the routing information of such large network topologies at each node and the updating process will be bandwidth consuming as it will be very frequent.

Some of these protocols depend only on the control messages that can be exchanged among the nodes for establishing a route and we call them *autonomous* protocols. Others depend on utilizing other navigation and traffic information sources for the route establishment and we call them *information-assisted* protocols. Examples of these navigation/traffic information sources are street maps, traffic maps, navigation software, traffic reports from RSUs, etc.

1) Autonomous Protocols

Some of these protocols depend on the exchange of periodic beacon packets (*beacon-based* protocols), while others do not (*beaconless* protocols).

- **Beacon-Based**

- The GPSR protocol [34] is a MANET protocol suggested for use in VANETs. It depends on the exchange of 1-hop periodic beacon messages carrying information about the sending node with the most important piece of information is the node's current position.
- Protocols depending on the exchange of traditional beacons suffer from the problem of inconsistency of the node's current position and the position announced in the beacon packet. This is because nodes keep moving and the information included in the beacon packets about their positions may be out-dated. The Greedy Perimeter Stateless Routing + Advanced Greedy Forwarding (GPSR+AGF) [66] solves this problem by letting nodes include extra information in the beacon packets about their speed, direction, and total travel time.
- The Greedy Routing with Abstract Neighbor Table (GRANT) protocol [67] depends on the idea of extended neighborhood knowledge where each node knows about its x-neighborhood. To avoid the overhead of exchanging x-hop neighbor information, GRANT divides the plane into areas and assigns only one representative for each area.
- The GpsrJ+ protocol [68] uses two-hop neighbor beaconing to provide broader view for the nodes taking decisions.
- The Connectivity-Aware Routing (CAR) protocol [69] follows the DSR approach for route discovery. It only discovers the path as a list of anchor points (nodes at junctions or road curves) and this list of anchor points is stored in the packets header.

- **Beaconless**

- The Contention-Based Forwarding (CBF) protocol [70] does not depend on exchanging periodic beacon packets among the neighboring nodes. It utilizes the concept of contention among the nodes and gives a priority of forwarding for only one node. In CBF, a node holding a packet broadcasts it to all its direct neighbors. Based on its distance to the destination, each node that receives the packet sets a timer for rebroadcasting the packet with the nearest node having the shortest timer. The actual forwarder is the nearest neighbor and the other potential forwarders are suppressed [71].

2) Information-Assisted Protocols

As mentioned above, these protocols import street or traffic information from external sources to help in forming more efficient routes. All the surveyed information-assisted protocols are also beacon-based ones. Examples are:

- The Geographic Source Routing (GSR) protocol [72] assumes the availability of city maps for its operation. It runs the selection algorithm on the map-based graph (i.e. the set of available junctions).
- In addition to utilizing static maps, the Anchor-based Street and Traffic Aware Routing (A-STAR) protocol [73] depends on the use of real-time traffic information. A-STAR utilizes two types of maps: a statically rated map (one based on stable bus routes) and a dynamically rated map (one based on real-time traffic conditions retrieved from monitoring RSUs) [71].

b) Route Selection

Most position-based routing protocols are based on the concept of greedy routing; a node holding a packet forwards it to the neighbor closest to the destination. Since the decision is done at the node getting the packet, route selection in the position-based greedy routing protocols is considered *intermediate-based*.

In making routing decision, protocols can be either *non-overlay* or *overlay based*:

1) Non-Overlay Based Protocols

In this category of routing, all nodes can be involved in the decision making process with equal roles and functionalities. Some of the protocols based on the non-overlay routing are:

- The GPSR and GPSR+AGF are examples of protocols utilizing the classic greedy routing approach for selecting the next forwarding node; picking the neighbor closest to the destination.
- The GRANT protocol depends on the use of extended greedy routing. As each node keeps information about it x-hop neighborhood, it has a new metric for selecting the next forwarding node.

2) Overlay Based Protocols

Overlay-based protocols depend on the use of representative nodes for the routing operation overlaid on top of the real network. These nodes have special roles and, in most cases, they are responsible for the routing decisions. In VANETs, these nodes are those at the junctions as junctions are the best places for making routing decisions as there are many options to follow there. Following are some of the functionalities utilized by the overlay-based protocols:

- The Greedy Perimeter Coordinator Routing (GPCR) protocol [74] utilizes the idea of greedy routing for forwarding packets along a road segment. When a packet reaches a junction, it stops there for deciding which road segment is best to follow. The reason behind that is preventing the packet from going to a wrong direction that will add extra unfavourable delay. It gives priorities to the nodes at the junctions (coordinators) as they have more available options and better view.

- The GpsrJ+ protocol does not restrict packets to stop at junctions. A node holding a packet my bypass the junction if it finds, by prediction, that nodes at the junction will forward the packet along the same direction.
- Some protocols depend on applying Dijkstra's algorithm for calculating the shortest path composed of a set of junctions from a source to a destination. An example is the GSR protocol. In GSR, the algorithm can be run only once with the list of selected junction points included in the packet header or the algorithm can be rerun at each forwarding node. Another example is the A-STAR protocol that, in calculating the shortest path, also considers the traffic density of the road segments.
- The Vehicle-Assisted Data Delivery (VADD) protocol [75] is designed for delay-tolerant VANETs. It is also based on using the junction points as decision making points. At each junction, vehicles choose the outgoing road with the lowest delay. Delay can be computed using a set of linear equations based on parameters such as road length, road density, and the average speed. After determining the next outgoing road, VADD has four variations for selecting the next forwarding node: 1) L-VADD: selects the closest node to the selected outgoing road regardless of its direction, 2) D-VADD: selects a node going toward the selected outgoing road regardless of its distance to it, 3) MD-VADD: selects multiple nodes going toward the selected outgoing road, ad 4) H-VADD: combines both L-VADD and D-VADD to reduce the delay incurred in D-VADD and avoid the potential loops of L-VADD [71].

These protocols utilize the greedy routing approach for forwarders selection between the junctions with the destination is the next junction point.

To determine the overlaid nodes (nodes located at junctions), there are many approaches introduced for the *autonomous* protocols:

- The GPCR protocol depends on the use of two heuristics:
  - If a node has two neighbors that do not list each other as neighbors while they are in the communication range of each other.
  - Depending on a correlation coefficient that relates each node to its neighbors. If the coefficient is close to 0, that means that there is no correlation among the node's neighbors, so, the node is at a junction.
- In the CAR protocol, a node is considered an anchor point if its velocity vector is not parallel to the one of the previous node in the packet.

The *information-assisted* protocols can get the set of junction points extracted from the streets map or retrieved from advanced navigation software.

There are few protocols that utilize the other types of route selection techniques. For example, the CAR protocol depends on the destination-based route selection technique for determining the list of anchor points toward the destination. If the destination receives multiple RREQs, it replies to the shortest one.

c) Route Representation and Data Forwarding

Most of VANETs position-based routing protocols are based on *route guidance* for data forwarding and they follow the self-routing approach; data forwarding decisions are made on the fly based on the neighbors and destination positions.

Few protocols utilize the *exact route* technique. As a part of the route representation of the overlay-based protocols, some protocols include the list of junction points in the packet header to follow. We can consider that a kind of *source routing*. So, these protocols utilize both source routing for representing the junction list and the greedy routing (based on *route guidance*) for data forwarding between two consecutive junctions.

d) Route Maintenance

Instead of handling failures of already established routes, route maintenance in VANETs involves handling failures of establishing routes due to intermittent connectivity.

It may happen that a node does not find a neighbor that is closer to the destination than the node itself. This case is known as reaching a *local maximum*. The routing protocol should include a mechanism for handling such situation by deploying a recovery mechanism. Many recovery mechanisms are introduced for the greedy protocols:

- The GPSR protocol recovers from a local maximum by entering the perimeter mode where it follows a mechanism known as the right-hand rule. This rule states that when a node enters the recovery mode, it forwards the data to the neighbor that is sequentially counterclockwise to the virtual line formed between the node in the recovery mode and the destination [71].
- The A-STAR technique for recovery from disconnectivity is recomputing the path to the destination from the stuck node with temporarily marking the disconnected part of the path to be “out of service”.
- The delay-tolerant protocols (e.g. VADD) recover from disconnections by having the stuck node storing the packet till having contact with another node. This approach is known as *store-carry-and-forward*.

The selection process returns to the greedy mode once the packet reaches a node that is closer to the destination than the node encountering the local maximum problem.

Also, because of the nodes high mobility, the information obtained and utilized in the beginning of the transmission may change and become invalid leading to disconnectivity. Therefore, protocols should utilize mechanisms for maintaining the route and network connectivity:

- The CAR protocol assumes that route disconnection is resulted from the destination movement[9]. It depends on the use of guard packets generated at the anchor points. When a destination changes its direction, it announces that to the nearest anchor point. When the data packet reaches the old destination’s location, it will be rerouted by the guarding nodes to the new estimated position.

In [76], B. Paul et al. presented a comparison among the well-known VANETs routing protocols by showing the pros and cons for each protocol.

3.3.5 Discussion

In this sub-section, we summarize the core components and functionalities providing a clear comparison between the routing functions of the four wireless multi-hop networks. The core components and functionalities of MANETs, WSNs, WMNs, and VANETs are illustrated in Figure 8, Figure 9, Figure 10, and Figure 11 respectively.

[9] It assumes that there is no disconnection problem among the anchor points.

As shown in the figures, there are some common functionalities for the various wireless multi-hop networks as they all share the same skeleton presented in Section 2. However, because each network paradigm has its own environmental features and requirements, there are some unique functionalities that distinguish each network paradigm from the other wireless multi-hop ones. These unique functionalities are added and utilized to assist the routing functions meet the paradigm and the application performance needs.

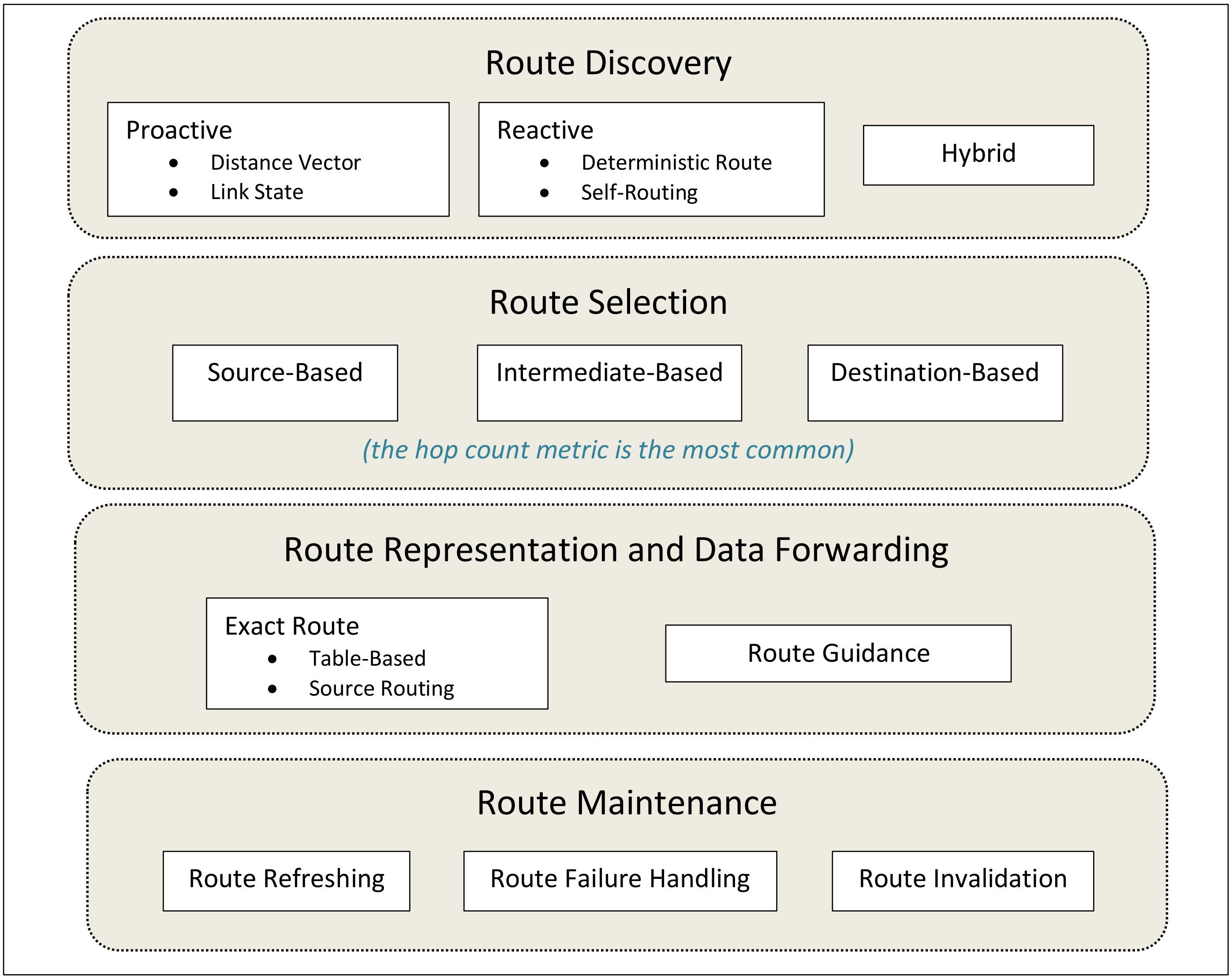

Figure 8 Core components and functionalities of MANET routing.

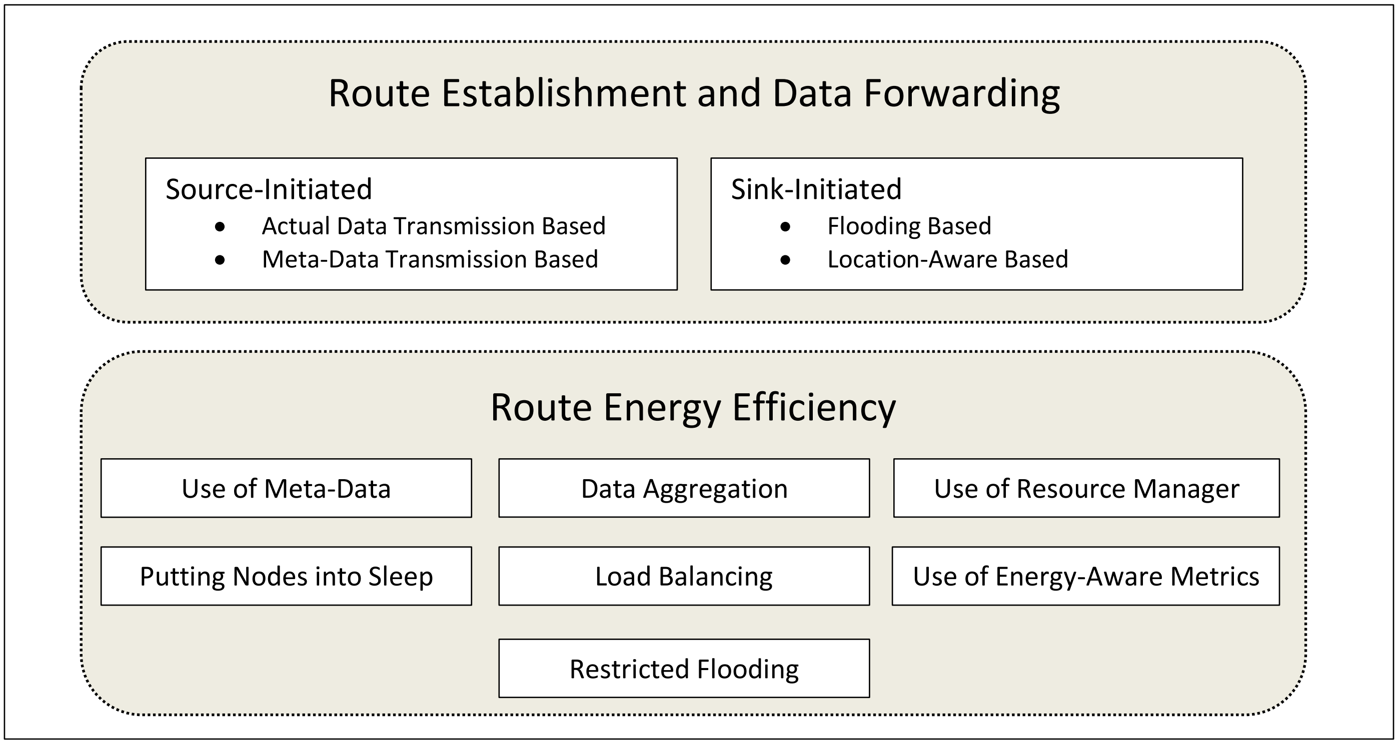

Figure 9 Core components and functionalities of WSN routing.

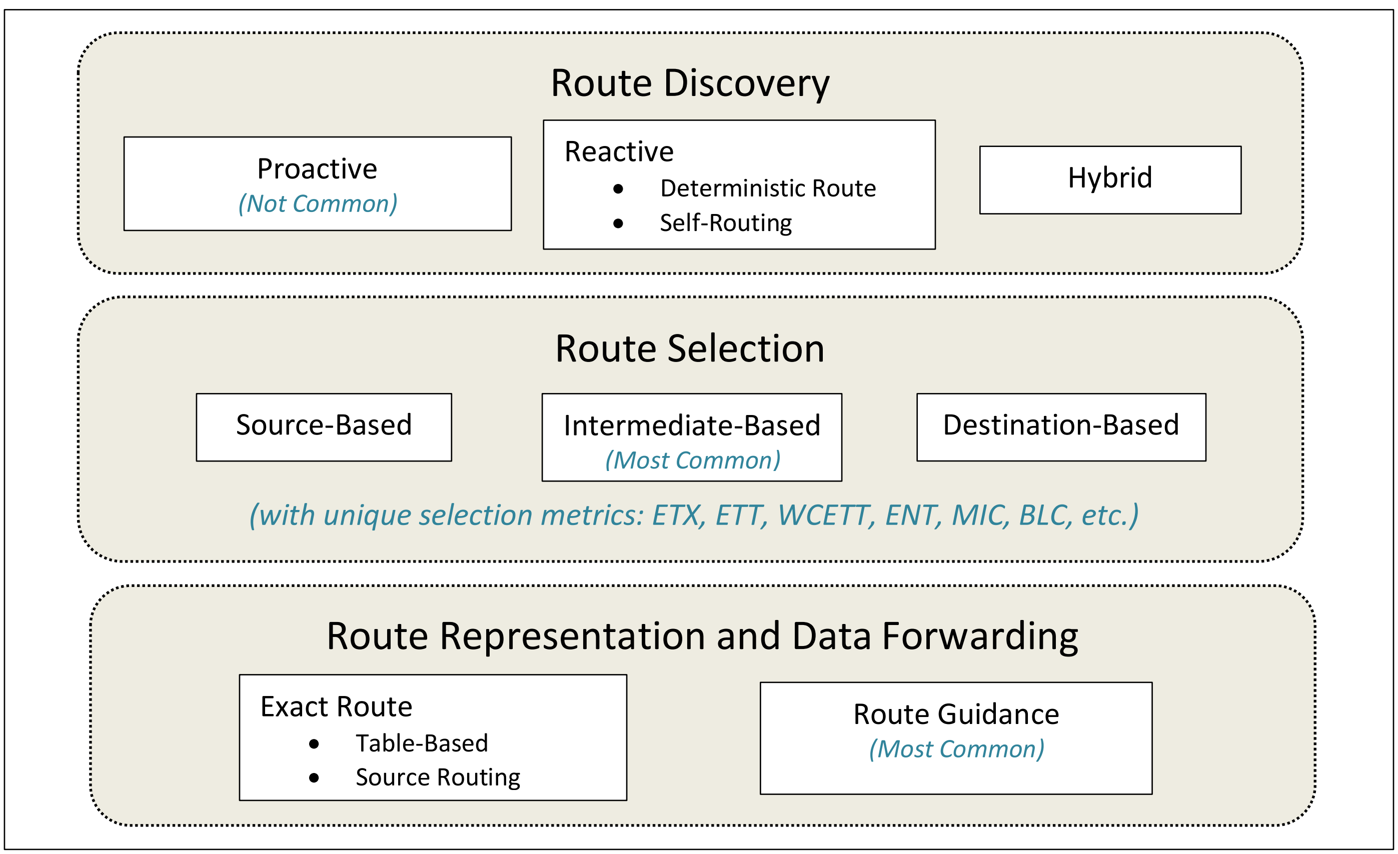

Figure 10 Core components and functionalities of WMN routing.

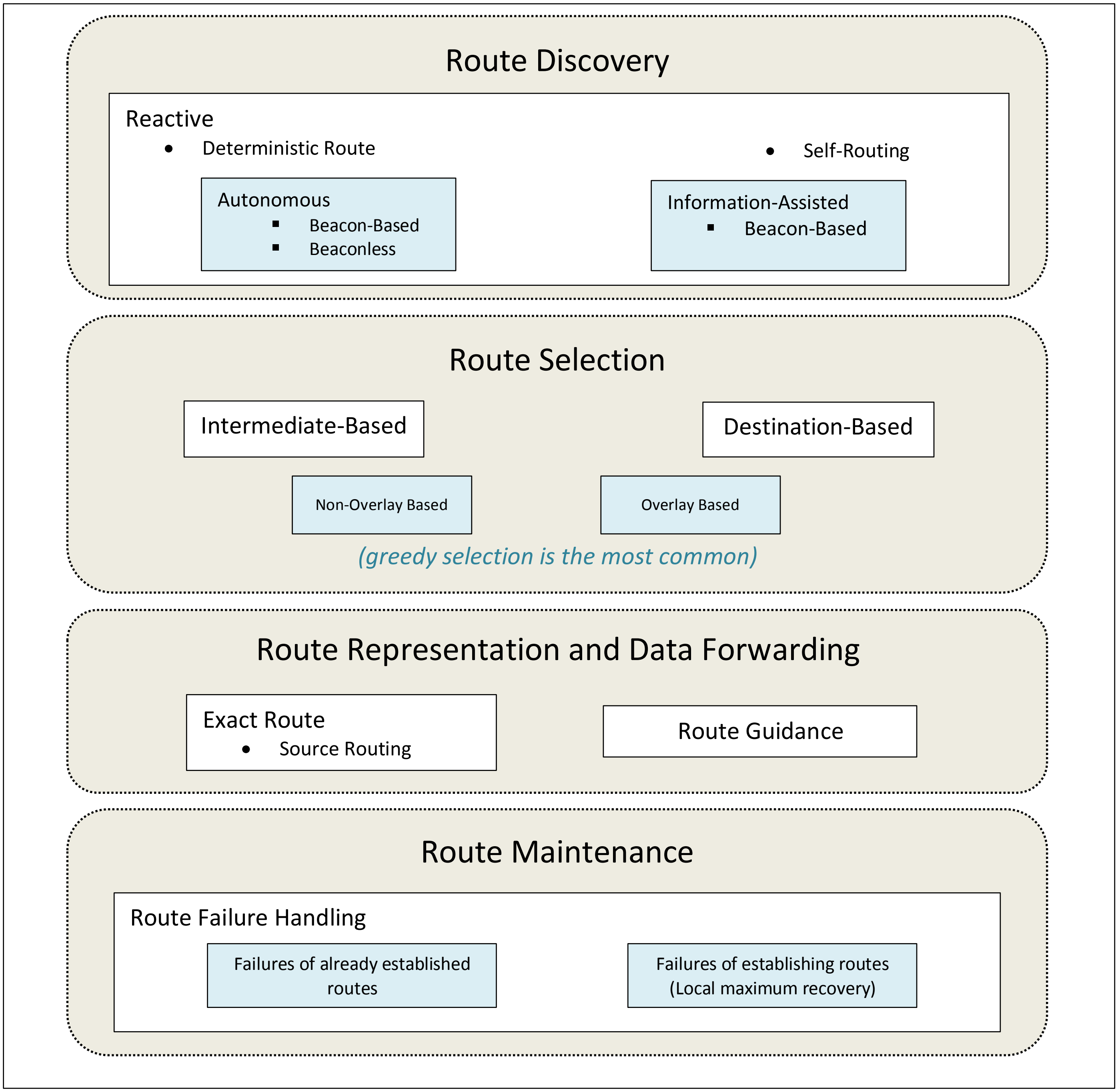

Figure 11 Core components and functionalities of VANET routing.

4 Conclusions and Open Issues

Throughout this paper, we have explored the various aspects related to routing in the wireless multi-hop networks; MANETs, WSN, WMNs, and VANETs. We have presented an introduction to routing, its basic functions, and how it fits in the protocol stack. We also explored the unifying features of the aforementioned networks by discussing the basic routing components that are main parts of any wireless multi-hop routing protocol and proposed a generic routing model that can be inherited in designing a wireless multi-hop routing protocol.

In addition, we have explored the various features that distinguish each network paradigm from the others. We have discussed the various challenges and characteristics, the most well-known routing taxonomy, the core routing components of each network paradigm for the sake of providing an extensive comparison between routing in the four wireless multi-hop networks.

Based on our surveys and studies for the various routing functionalities and protocols of the wireless multi-hop networks, we have reached a conclusion about the ideal routing protocol that provides the optimum operation with efficient utilization of the network resources. We have concluded that the *self-routing* approach will be the dominant one for all the network paradigms since self-routing has a great advantage in adapting to changes in the links status and connectivity.

In MANETs, instead of keeping a deterministic route, doing routing on the fly (i.e. hop-by-hop) helps in handling links failures and disconnectivity; hence, saving the time and the bandwidth wasted in the route maintenance mechanisms and discovery of alternative routes.

In WSNs, self-routing helps in handling node failures resulted from either energy depletion or harsh environmental damage. By selecting the path on the fly, it is ensured that there will be a connected path to the destination. In addition, hop-by-hop routing helps in balancing the load among the various potential forwarders; hence, energy consumption will be well-balanced among the nodes.

In WMNs, it is observed that the best functionality is the one done hop-by-hop as this technique adapts to the links status changes. Wireless links are subject to changes in their bandwidth, interference level, etc. The effects of such changes can be mitigated if the route establishment is done on the fly instead of having it deterministic. So, self-routing helps in tackling the short-term path quality variations problem of WMNs.

In VANETs, the most popular routing protocols are the self-routing ones as they are the best handlers for the intermittent connectivity and dynamic topology.

Derived from the summarizing figures presented in the previous section, Figure 12 illustrates the ideal model and its ideal functionality per each component.

Self-routing requires that route discovery is handled in a *reactive* way, route selection should be *intermediate-based*, and the route representation and data forwarding is done based on *route guidance.*

For the selection metric, each network paradigm should have its own metric based on the goals and needs of each paradigm. MANETs can have the ***mobility level*** as its selection metric. Choosing the most stable neighbor (the slowest one) to be the next forwarding node reduces the probability of route failures due to links changes. For WSNs, the selection metric can be the ***residual energy*** of the potential forwarders. Choosing the neighbor with the highest residual energy reduces the opportunity to nodes' batteries depletion. In WMNs, there are different selection metrics that can be utilized and are suitable for the intermediate-based selection. These metrics are discussed in Table 2 and we can refer to them here as ***QoS level*.** Finally, the most popular self-routing based VANETs protocols are based on greedy selection; in other words, the selection metric for VANETs should be the ***distance to the destination***.

So, by combining the functionalities shown in Figure 12 and choosing the suitable selection metric, an ideal wireless multi-hop routing protocol can be designed.

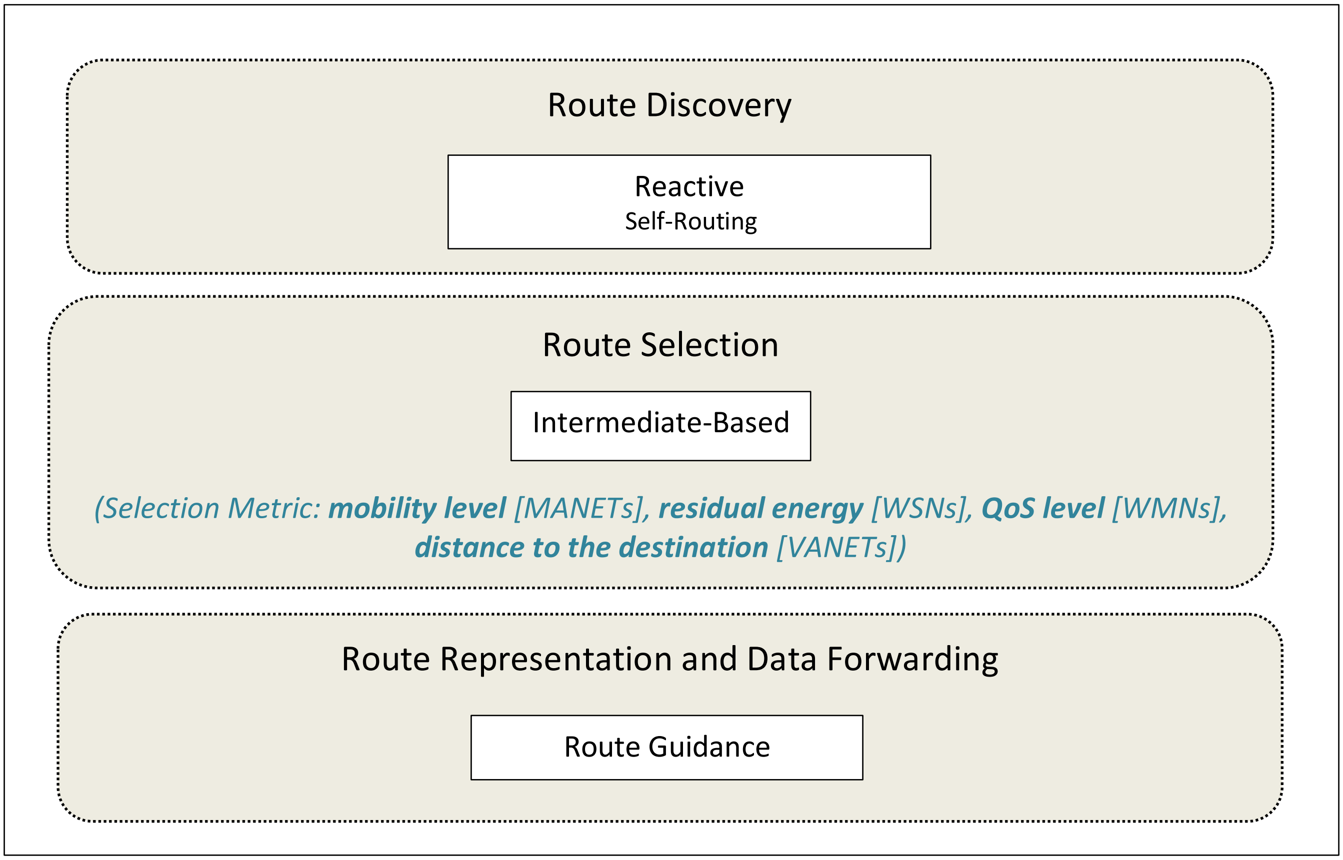

Figure 12 Ideal Routing Model.

For future work in the area of wireless multi-hop routing, our proposal for the ideal protocol can be considered, inherited, and enhanced. Also, a super routing protocol that can fit all wireless multi-hop networks can be proposed based on this view of the ideal routing protocol.

As we have seen throughout this document, a considerable number of routing protocols have been proposed for the various wireless multi-hop networks. With these protocols available in the literature, there are still many open issues that need to be covered in the area of wireless multi-hop routing. Most of the open issues are related to WMNs and VANETs considering that these are the most recent wireless multi-hop network paradigms.

Although there are tens of WMN routing protocols in the literature, there are still some open issues need to be covered to improve the efficiency of the WMN routing function: ***1)*** Extensive testing for the various routing metrics is needed to pick up the most accurate and efficient metric or a combination of metrics, ***2)*** Proposing passive techniques for measuring metrics parameters instead of depending on exchanging control packets for the sake of reducing the overhead and utilizing network resources efficiently, ***3)*** Studying the impact of the active measurements techniques on increasing the self-interference problem, ***4)*** Many protocols depend on the use of the Dijkstra algorithm for calculating the best path. The use of such algorithm hinders the network scalability. Other approaches should be investigated for the optimal path computation, ***5)*** Further exploration for the impact and the benefits of the network coding strategies. Currently, only few WMN routing protocols utilize this coding opportunities [60].

For VANETs, although there are many new protocols introduced for routing functionalities, routing is still considered one of the hottest topics in the VANETs research area. There are some open issues and opportunities that can be handled and considered by the researchers to improve the performance of messages routing and pave the road to many new applications and services to be supported by VANETs communications, among them: ***1)*** Most of VANETs routing protocols depend on the greedy selection which just considers the distance to the destination. This approach for routing selection lacks considering some real physical conditions such as fading and interference which may affect reception of the packets by the selected recipient. Other selection metrics should be taken into consideration to provide more efficient routing decisions. Such metrics can be merged with the greedy approach by optimization solutions, ***2)*** As VANETs application will include real time communications for; for example, sharing videos and playing games on the move among passengers of many neighboring vehicles, QoS support should be considered by new VANETs routing protocols to satisfy the requirements of these types of communications, ***3)*** With the advances of the built-in VANETs communication modules, many interfaces and technologies will be available for transmitting the packets. The availability of these multiple radios and technologies should be considered by the routing protocols to provide the most efficient transmission over the highly available commination technology, ***4)*** Routing should be aware of the higher-layers requirements and generated traffic to better assist the application operation. This leads to what is known as content-based routing, in which, the contents of the messages should be taken into consideration for providing the optimal routing functionalities and decisions. For example, in a case of an accident or health emergency, packets should be routed to the nearest ambulance in addition to the neighboring vehicles, ***5)*** One of the most enabling factors in VANETs communication is the inclusion of the infrastructure. Most of the VANETs routing protocols ignore the infrastructure exploitation for the messages transmission. Depending on the infrastructure can help in handling the intermittent connectivity and expediting the transmission time; hence, reducing the delay. So, routing protocols that exploit the existence of the infrastructure need to be proposed, ***6)*** Network coding can be considered as an efficient mechanism of reducing the number of transmissions and utilizing network resources efficiently, ***7)*** the number of delay-tolerant routing protocols is limited compared to the non-delay-tolerant ones. So, further research is need to be investigated in the area of routing for delay-tolerant VANETs, ***8)*** As VANETs can operate in many various scenarios and traffic conditions and support different applications, VANETs routing protocols should be adaptable to these different application requirements and be scalable to various network sizes in different times of the day [15].

In addition, as a common opportunity for all wireless multi-hop networks, the introduction of the cognitive radios and its integrations with the wireless multi-hop networks will open many research issues for the wireless multi-hop routing area of research. Cognitive radios add some challenges with its intermittent connectivity and bandwidth availability that should be handled and taken into consideration with the routing functions [60].

In short, many wireless multi-hop routing protocols are available in the literature, and, although they have some common and unifying features, they also have their own distinguishing ones based on the network paradigm they are proposed for. Some hot open issues and opportunities are also available for the interested researchers to work on.

References

[1] S. Basagni, M. ContI, S. Giordano, and I. Stojmenovic, *Mobile Ad Hoc Networking*.: IEEE PRESS, John Wiley & Sons, Inc., 2004.

[2] M. J. Lee, J. Zheng, X. Hu, H. Juan, Ch. Zhu, Y. Liu, J. S. Yoon, and T. N. Saadawi, "A New Taxonomy of Routing Algorithms for Wireless Mobile Ad Hoc Networks: The Component Approach," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 116-123, November 2006.

[3] A. S. Tanenbaum, Computer Networks, 4th ed.: Prentice Hall, 2003.

[4] E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs," in Numerische Mathematik 1, 1959, pp. 269 - 271.

[5] S. Mueller, R. Tsang, and D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges," in Performance Tools and Applications to Networked Systems, volume 2965 of LNCS, Springer-Verlag, 2004.

[6] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-based Routing in Mobile Ad-hoc Networks," IEEE Network Magazine 15 (6), 2001, pp. 30–39.

[7] D. A. Johnson and D. B. Maltz, "Dynamic Source Routing in in Ad Hoc Wireless Networks," in Mobile Computing, (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ., 1996, pp. 153-181.

[8] J. Jubin and J. Tornow, "The DARPA Packet Radio Network Protocols," in Proc. IEEE, vol. 75, no. 1, 1987, pp. 21–32.

[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a survey," Elsevier's Computer Networks, vol. 38, no. 4, pp. 393 – 422, Mar. 2002.

[10] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks Journal, vol. 47, no. 4, pp. 445–487, 2005.

[11] J. Jun and M.L. Sichitiu, "MRP: Wireless Mesh Networks Routing Protocol," Comput. Comm., 2008.

[12] H. Hartenstein and K. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communications Magazine, 46(6), 2008.

[13] "Status of Project IEEE 802.11 Task Group p" http://grouper.ieee.org/groups/802/11/Reports/tgp_update.htm. Retrieved December 06, 2011.

[14] E. Schoch, F. Kargl, and M. and Weber, "Communication Patterns in VANETs," IEEE Communications Magazine, vol. 46, pp. 119-125, November 2008.

[15] F. Ros, V. Cabrera, J. Sanchez, J. Martinez, and P. Ruiz, "Routing in Vehicular Networks," in Vehicular Networks: Techniques, Standards, and Applications, H. Moustafa and Y. Zhang, Eds. Boston, MA: Auerbach Publications, 2009.

[16] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," in IEEE Wireless Communications, Volume 11, Issue 6, Dec. 2004.

[17] Z. Jin, Y. Jian-Ping, Z. Si-Wang, L. Ya-Ping, and L. Guang , "A Survey on Position-Based Routing Algorithms in Wireless Sensor Networks," in Algorithms , 2, 2009, pp. 158-182.

[18] I.F. Akyildiz and X. Wang, Wireless Mesh Networks. Chichester, United Kingdom: John Wiley & Sons Ltd., February 2009.

[19] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, “Routing in Sparse Vehicular Ad Hoc Wireless Networks,” in IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1538–1556, Oct. 2007.

[20] P. Luo, H. Huang, W. Shu, M. Li, and M.-Y. Wu, “Performance Evaluation of Vehicular DTN Routing Under Realistic Mobility Models,” in Proc. IEEE Wireless Communications and Networking Conference 2008 (WCNC’08), pp. 2206-2211, April 2008.

[21] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers," in ACM Computer Communication Review, Vol. 24, No.4, (ACM SIGCOMM’94), Oct. 1994, pp. 234-244.

[22] S. Murthy and J.J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, pp. 183-97, Oct. 1996.

[23] G. Pei, M. Gerla and T.-W. Chen, “Fisheye State Routing in Mobile Ad Hoc Networks,” in Proc. 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78.

[24] P. Jacquet, P. Muhlethaler, and A. Qayyum, “Optimized Link State Routing Protocol,” IETF MANET, Internet draft, 1998.

[25] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. WoodWard, “A Distance Routing Effect Algorithm for Mobility (DREAM),” in Proc. 4th MOBCOM, 1998.

[26] C. C. Chiang, T. C. Tsai, W. Liu, and M. Gerla, “Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel,” in Proc. IEEE SICON'97, Apr. 1997, pp. 197-211.

[27] R. Sivakumar, P. Sinha, and V. Bharghaven, “CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm,” IEEE Journal on Selected Areas in Communications, vol.17, no.8, pp.1454-1465, Aug. 1999.

[28] C.E. Perkins and E.M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in 2nd IEEE Workshop of Mobile Computing systems and applications, WMCSA ’99, Feb. 1999, pp. 90–100.

[29] Y. B. Ko and N. H. Vaidya, “Location Aid Routing (LAR) in mobile ad hoc networks,” in Wirel. Netw. J., vol. 6, July 2000, 307-321.

[30] Z. J. Haas and M.R Pearlman, "The Zone Routing Protocol (ZRP) for ad hoc networks," IETF Internet draft, Aug. 1998.

[31] M. Joa-Ng and I-Tai Lu, “A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks,” IEEE on Selected Areas in Communications J., vol.17, no.8, pp.1415-1425, Aug 1999.

[32] A. Zhou and H. Hassanein, "Load-Balanced Wireless Ad Hoc Routing," in Proc. Canadian Conference on Electrical and Computer Engineering, vol.2, pp.1157-1161, 2001.

[33] H. Du, H. Hassanein, and C. Yeh, "Zone-Based Routing Protocol for High-Mobility MANET," in Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE’03), vol.2, pp. 1055- 1058, May 2003.

[34] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Proc. International Conference on Mobile Computing and Networking (MobiCom'00), pp. 243-254, 2000.

[35] J. Mingliang, L. Jinyang, and Y. C. Tay, "Cluster Based Routing Protocol (CBRP)," IETF MANET, Internet draft, 1999.

[36] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in Proc. INFOCOM '97, vol. 3, Apr.1997, pp. 1405 -1413.

[37] Ch. Liu and J. Kaiser, "A Survey of Mobile Ad Hoc Network Routing Protocols," Department of Computer Structures - University of Ulm, Germany, Tech. rept. 2003-08, October 2003.

[38] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks," in IEEE Computer Society Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000.

[39] F. Ye, A. Chen, S. Lu, and L. Zhang, "A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks," in Proc. 10th Int'l. Conf. Comp. Commun. and Networks, 2001, pp. 304–09.

[40] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," Proc. IEEE Aerospace Conf., 2002, vol. 3, 9–16, pp. 1125–30.

[41] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," in Proc. 5th ACM/IEEE Mobicom, Seattle, WA, Aug. 1999. pp. 174–85.

[42] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks," in ACM MobiCom'00, Boston, MA, Aug. 2000, pp. 56-67.

[43] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in Proc. 1st Workshop of Sensor Networks and Apps., Atlanta, GA, Oct. 2002.

[44] C. Schurgers and M.B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," in Proc. Military Communications Conference (MILCOM'01), McLean, VA, 2001.

[45] H. Hassanein and J. Luo, "Reliable Energy Aware Routing In Wireless Sensor Networks," in Proc. 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS'06) , pp.54-64, April 2006.

[46] Y. Yao and J. Gehrke, "The Cougar Approach to In-network Query Processing in Sensor Networks," SIGMOD Record, vol. 31, no. 3, Sept. 2002.

[47] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," in IEEE Wireless Communications, vol. 11, no. 6, Dec. 2004.

[48] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," Univ. California, Los Angeles, UCLA/CSD-TR-01-0023, 2001.

[49] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," in Proc. IEEE Wireless Communications and Networking Conference (WCNC'02), Orlando, FL, vol.1, pp. 350- 355, Mar. 2002.

[50] B. Wehbi, W. Mallouli, and A. Cavalli, “Light Client Management Protocol for Wireless Mesh Networks,” in Proc. 7th International Conference on Mobile Data Management (MDM’06), pp. 123–126, May 2006.

[51] R. Draves, J. Padhye, and B. Zill, "Comparisons of Routing Metrics for Static Multi-Hop Wireless Networks," in ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM), 2004, pp. 133–144.

[52] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), 2004, pp. 114–128.

[53] B. Cheng, M. Yuksel, and S. Kalyanaraman, “Orthogonal Rendezvous Routing Protocol for Wireless Mesh Networks,” in Proc. IEEE International Conference on Network Protocols (ICNP’06), pp. 106–115, 2006.

[54] K. N. Ramachandran, M.M. Buddhikot, G. Chandranmenon, S. Miller, K. C. Almeroth and E. M. Belding-Royer, "On The Design and Implementation of Infrastructure Mesh Networks," in IEEE Workshop on Wireless Mesh Networks (WIMESH), 2005.

[55] Z. Wu, S. Ganu, and D. Raychaudhuri, “IRMA: Integrated Routing and MAC Scheduling in Multihop Wireless Mesh Networks,” in Proc. IEEE Workshop on Wireless Mesh Networks (WIMESH’06), Reston, VA, Sept 2006, pp. 1–8.

[56] M. Campista, P. Esposito, I. Moraes, L. Costa, O. Duarte, D. Passos, C. de Albuquerque, D. Saade, and M. Rubinstein, "Routing Metrics and Protocols for Wireless Mesh Networks," IEEE Network, vol. 22, no. 1, pp. 6-12, Jan. 2008.

[57] C.E. Koksal and H. Balakrishnan, “Quality-aware Routing Metrics for Time-varying Wireless Mesh Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 11, pp. 1984–1994, Nov. 2006.

[58] Y. Yang, J. Wang, and R. Kravets, "Interference-aware Load Balancing for Multihop Wireless Networks," Department of Computer Science, University of Illinois, Urbana-Champaign, Tech. Rep. UIUCDCS-R-2005-2526, 2005.

[59] T. Liu and W. Liao, “Capacity-aware Routing in Multi-channel Multi-rate Wireless Mesh Networks,” in Proc. IEEE International Conference on Communications (ICC’06), Istanbul, pp. 1971–1976, June 2006.

[60] J. Núñez-Martínez and J. Mangues-Bafalluy, “A Survey on Routing Protocols that really Exploit Wireless Mesh Network Features,” in Journal of Communications, vol. 5, no. 3, March 2010.

[61] N.S. Nandiraju, D.S. Nandiraju, and D.P. Agrawal, "Multipath Routing in Wireless Mesh Networks," in IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS’06), Vancouver, BC, 2006, pp. 741–746.

[62] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," in ACM SIGCOMM, Aug. 2005, pp. 133–144.

[63] Y. Yuan, H. Yang, S. H. Y. Wong, S. Lu, and W. Arbaugh, "ROMER: Resilient Opportunistic Mesh Routing for Wireless Mesh Networks," in 1st IEEE Workshop on Wireless Mesh Networks (WiMesh’05), Sept. 2005.

[64] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," ACM SIGCOMM Comput. Commun. Rev. 37, no. 4, pp. 169-180, Oct. 2007.

[65] J. Le, J. Lui, and D.-M. Chiu, "DCAR: Distributed Coding-Aware Routing in Wireless Networks," in IEEE Transactions on Mobile Computing, vol.9, no.4, pp.596-608, April 2010.

[66] V. Naumov, R. Baumann, T. Gross, "An Evaluation of Inter-Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces," in Proc. ACM MobiHoc'06 Conf., May 2006.

[67] S. Schnaufer and W. Effelsberg, "Position-based Unicast Routing for City Scenarios," International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM'08), pp.1-8, June 2008.

[68] K. C. Lee, J. Haerri, U. Lee, and M. Gerla, "Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios," IEEE Globecom Workshops, pp. 1–10, Nov. 2007.

[69] V. Naumov and T.R. Gross, "Connectivity-Aware Routing (CAR) in Vehicular Ad-hoc Networks," in Proc. 26th IEEE International Conference on Computer Communications (INFOCOM'07), pp.1919-1927, May 2007.

[70] H. F¨ußler, H. Hannes, W. J¨org, M. Martin, and E. Wolfgang, "Contention-Based Forwarding for Street Scenarios," in Proc. 1st International Workshop in Intelligent Transportation (WIT'04), pp. 155–160, Hamburg, Germany, March 2004.

[71] K. Lee, U. Lee, and M. Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks," in Advances in Vehicular Ad-Hoc Networks: Developments and Challenges.: IGI Global, 2009.

[72] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A Routing Strategy for Vehicular Ad Hoc Networks in City Environments," in Proc. IEEE Intelligent Vehicles Symposium, pp. 156-161, June 2003.

[73] B.-C. Seet, G. Liu, B.-S. Lee, C. H. Foh, K. J. Wong, and K.-K. Lee, "A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications," in Proc. NETWORKING 2004, pp. 989-999.

[74] C. Lochert, M. Mauve, H. F¨ussler, and H. Hartenstein, "Geographic Routing in City Scenarios," SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 1, pp. 69–72, 2005.

[75] J. Zhao and G. Cao, "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad hoc Networks," IEEE Transactions on Vehicular Technology, vol. 57, no. 3, pp. 1910-1922, 2008.

[76] B. Paul, M. Ibrahim, and M. A.N. Bikas, "VANET Routing Protocols: Pros and Cons," in the International Journal of Computer Applications, vol. 20, no. 3, Apr. 2011.