ISSN: 2277-5528
Impact Factor: 5.085

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

MESSAGE FORWARDING IN OPPORTUNISTIC NETWORK USING PROPHATE PROTOCOL

Rameshwar Singh Sikarwar, Rahul Sharma
Department of Computer Application, Dr. APJ Abdul Kalam University, Indore (M.P.)

ABSTRACT

In opportunistic networks, route connecting to the mobile nodes never exists, mobile nodes communicates with each other when they get opportunity to communicate. Furthermore, nodes are not supported to posses or acquire any knowledge about the network topology. Rotes are built dynamically, while messages are route between the source and the destination and any possible node can opportunistically be used as next hope, provided it is likely to bring the message closer to the final destination. These requirements make opportunistic networks a challenging and promising research field.

Opportunistic mobile ad hoc networks consist of human-carried mobile devices that communicate with each other in a store-carry-forward fashion, without any infrastructure. They present distinct challenges compared to classical networks, such as the Internet, that assumes the availability of a contemporaneous, reasonably low propagation delay, low packet loss rate path between the two end points that communicate. In opportunistic networks, disconnections and highly variable delays caused by human mobility are the norm. Another major challenge in opportunistic communications arises from the small form factor of mobile devices which introduces resource limitations compared to static computing systems. Moreover, implementation and deployment of actual opportunistic mobile networks, systems and applications is challenging, very often expensive and time-consuming. Hence, the research community has mainly relied on simulations and analytical modeling, or on simple proof of concept prototypes to demonstrate the feasibility of these systems.

This research is concerned with hybrid approach for routing in opportunistic networks, rendering traditional routing protocols unable to deliver messages between hosts. Thus, there is a need for a way to route through such networks. We propose hybrid approach which combines Epidemic Routing and Probabilistic Routing approaches together. This protocol improves reliable message delivery and low overhead on resources.

Introduction

With the proliferation of a variety of wireless access technologies, seamless connectivity and anywhere, anytime computing are commonly touted as the paradigms for serving mobile users. Further, broadband wireless access is described as the panacea for the last-mile problem. While the vision of seamless connectivity and broadband wireless Internet access is attractive, it is far from reality. For various regulatory, technical and economical reasons, wireless access networks worldwide fail to fulfill the promise of continuous, high-bandwidth, and affordable service.

Cellular networks (e.g., GSM/UMTS) are the most common option for mobile wide-area network access. Their coverage continues to be variable and intermittent. In terms of performance, 2/2.5G networks provide low bandwidth access. While 3G promises high bandwidth access, it is expensive and its metered service is not viewed as a true option for extensive Internet access. The potential success of newer technologies using licensed spectrum such as IEEE 802.16 (WiMax) remains questionable [2]. The substantial investment made in 3G licenses and infrastructure is a deterrent for network operators to adopt a new technology for mobile broadband access. As a broadband solution to the last-mile problem in poor and developing countries and in rural and remote areas, Wi-Max and other licensed wireless access technologies face the chicken-and-egg problem of the simultaneous need for both a market and an infrastructure. Providing continuous broadband coverage in rural areas can be an expensive endeavor for network operators due to the sparse population density, e.g. [2], challenging terrain, and lack of other relevant infrastructure such as reliable supply of electricity [2]. IEEE 802.11 (Wi-Fi) has experienced widespread proliferation thanks to its operation in the unlicensed spectrum and cheap hardware. But coverage of Wi-Fi hotspots is limited to few hundred meters.

In spite of efforts to extend the coverage of infrastructure wireless networks, for instance, using the multi-hop ad-hoc and mesh networking approach, intermittent connectivity prevails. Still, wireless access networks today are architect for providing continuous, synchronous access to users; to a great extent this can be attributed to the end-to-end communication paradigm prevalent in the Internet. Irrespective of the kind of network services a user is interested in, the end-user is expected to be physically present within the coverage of these infrastructure based access networks for any communication to take place. This I believe is a major hurdle for extending network access to a sizeable user population who cannot afford to be physically present within the coverage area of the nearest base station or hotspot and to mobile users who find it cumbersome keeping track of their intermittent network access as they move in and out of the sporadic coverage. While continuous, connectivity is essential for synchronous applications such as real-time video and voice conferencing, there are many asynchronous applications: cached Web access, electronic mail, multimedia messaging, news casting, file sharing, and blogging, to name a few that do not need continuous network access. But today‛s networks and protocols are not resilient to disruption of communication links, and are not designed to exploit intermittent availability of network resources. Communication opportunities in a network can arise in different forms. They can be:

- Deterministic periodic connectivity, e.g., in an interplanetary network based on the movement patterns of planets and satellites, or connectivity that is a function of time synchronization among sensors.
- Coordinated a group of users deciding to meet at a particular location at a certain time to share data.
- Spontaneous when two or more devices meet by chance, e.g., two or more users with common interests meeting at an airport.

WIRELESS AD HOC NETWORKS

A wireless ad-hoc network is a decentralized type of wireless network [4]. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks

Ad hoc networks, which are also called *mesh networks*, are defined by the manner in which the network nodes are organized to provide pathways for data to be routed from the user to and from the desired destination [19]. Actually, the two names described to these networks provide considerable insight. *Ad hoc* has two definitions—the first can be either —impromptu‖ or —using what is on hand,‖ while the other is —for one specific purpose.‖ For example, members of an ad hoc committee (studying a specific issue) might discover that they are attending the same event and decide to have an ad hoc (impromptu) meeting. Ad hoc networks follow both definitions, as well. They are formed as they are needed (impromptu), using resources on hand, and are configured to handle exactly what is needed by each user—a series of —one specific purpose‖ tasks. The term mesh network accurately describes the structure of the network: All available nodes are aware of all other nodes within range. The entire collection of nodes is interconnected in many different ways, just as a physical mesh is made of many small connections to create a larger fabric. Figure 3.1 provides a simple diagram illustrating these concepts. This diagram is modeled after a wireless —hot spot,‖ where an ad hoc network links users to a router with access tothe Internet. In this example, two users are highlighted, showing two paths through several nodes to the router.

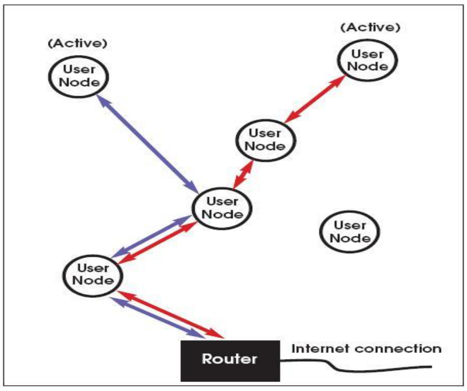


Figure 3.1: Basic structure of an ad hoc, or mesh, network. The path from the user's node to the destination ode is provided by other users' devices acting as routers.

If one of the intermediate nodes were to fail (e.g. that user leaves the area), the network will automatically reconfigure itself, locating an alternate path from the user to the router. Typically, all available nodes are also network users, each sharing the total data transfer capacity of the particular hardware and operating protocol being used. The network could also connect users to other users directly, as would be done in an industrial control and monitoring network. Since there is no need for central administration of the network configuration, it is most efficient to design the system for autonomous operation of each node. In an industrial environment, a situation such as an alarm would be propagated through the network and received directly by each node. Each node would be programmed to respond according to its particular function— machine control, process monitoring, supervisory personnel or central office.

Advantages of Ad Hoc Networks

The principal advantages of an ad hoc network include the following:

- Independence from central network administration
- Self-configuring, nodes are also routers
- Self-healing through continuous re-configuration
- Scalable—accommodates the addition of more nodes
- Flexible—similar to being able to access the

Internet from many different locations

Limitation of Ad Hoc Networks

While ad hoc networks are typically used where they have the greatest emphasis on its advantages, there are some limitations:

- Each node must have full performance
    - Throughput is affected by system loading
    - Reliability requires a sufficient number of available nodes. Sparse networks can have problems
    - Large networks can have excessive latency (time delay), which affects some applications

Some of these limitations also apply to conventional hub-and-spoke based networks, or cannot be addressed by alternate configurations. For example, all networks are affected by system loading, and networks with few nodes are difficult to justify in hard-wired solutions.

MOBILE AD – HOC NETWORK (MANET)

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad hoc is Latin and means ―for this purpose‖ [18]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

As the importance of computers in our daily life increases it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting to the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected). This is where ad hoc networks step in. In Latin, ad hoc means "for this," further meaning "for this purpose only. It is a good and emblematic description of the idea why ad hoc networks are needed. They can be set up anywhere without any need for external infrastructure (like wires or base stations). They are often mobile and that's why a term MANET is often used when talking about Mobile Ad hoc NETworks [22]. MANETs are often defined as follows: A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links - the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. The strength of the connection can change rapidly in time or even disappear completely. Nodes can appear, disappear and re-appear as the time goes on and all the time the network connections should work between the nodes that are part of it. As one can easily imagine, the situation in ad hoc networks with respect to ensuring connectivity and robustness is much more demanding than in the wired case. Ad hoc networks are networks are not (necessarily) connected to any static (i.e. wired) infrastructure. An ad-hoc network is a LAN or other small network, especially one with wireless connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

The ad hoc network is a communication network without a pre-exist network infrastructure. In cellular networks, there is a network infrastructure represented by the base-stations, Radio network controllers, etc. In ad hoc networks every communication terminal (or radio terminal RT) communicates with its partner to perform peer to peer communication. If the required RT is not a neighbor to the initiated call RT (outside the coverage area of the RT), then the other intermediate RTs are used to perform the communication link. This is called multi-hope peer to peer communication. This collaboration between the RTs is very important in the ad hoc networks. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals (i.e. the communication terminals should be independent and highly cooperative).

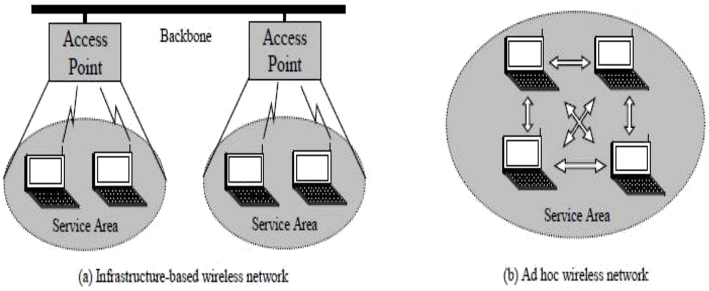

Access Point
Backbone
Access Point
Service Area
Service Area
Service Area
(a) Infrastructure-based wireless network
(b) Ad hoc wireless network

Figure 1: Infrastructured and infrastructureless wireless networks.

MANET Feature

MANET has the following features:

I. ***Autonomous terminal***. In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

II. ***Distributed operation***. Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

III. ***Multihop routing***. Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

IV. ***Dynamic network topology***. Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming theirown network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network but may require access to a public fixed network (e.g. Internet).

V. ***Fluctuating link capacity*.** The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

VI. ***Light-weight terminals.*** In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

VEHICULAR AD – HOC NETWORKS (VANET)

Vehicular Ad-Hoc Networks (VANET) is becoming an integral technology for connecting daily life to computer networks. They could greatly improve the driving experience both in terms of safety and efficiency. As shown in Figure 5.1, when multi-hop communication is implemented, VANET enables a vehicle to communicate with other vehicles which are out of sight or even out of radio transmission range. It also enables vehicles to communicate with roadside infrastructure. VANET will likely be an essential part of future Intelligent Transportation Systems (ITS) [23].

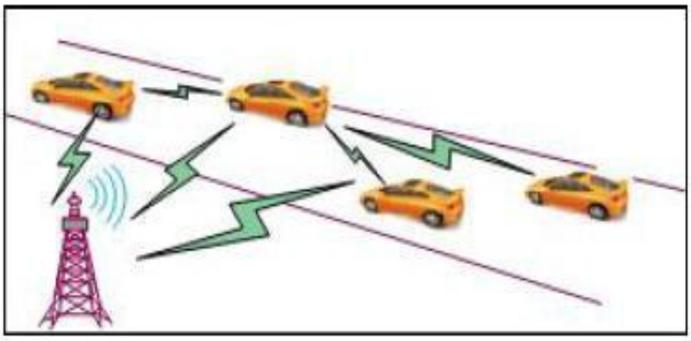


Figure 2: Vehicular ad-hoc networks.

Currently, ITS relies heavily on infrastructure deployment. Electromagnetic sensors, for example, are embedded into the road surface; traffic cameras are deployed at major intersections; and Radio Frequency Identification (RFID) readers are deployed at highway entrances. A typical procedure for collecting and distributing traffic information is as follows. First, traffic samples are gathered by road surface sensors and uploaded to a municipal transport center. After data processing, traffic reports can then be delivered to a user‘s cell phone via cellular networks. This is an expensive and inefficient way of disseminating location-based information, especially when the information of interest is only a few hundred meters from the user‘s physical location. With its short-range communication capabilities, VANET may change this paradigm and make generating and disseminating information more straightforward.

VANET can also serve as a large-scale wireless sensor network for future ITS because every modern vehicle can be regarded as a super sensor node. For example, all new vehicles are usually equipped with exterior and interior thermometers, light sensors, one or more cameras, microphones, ultrasound radar, and other sensory features. Moreover, future vehicles will also be equipped with an on-board computer, wireless radio, and a GPS receiver, which will enable them to communicate with each other and with roadside units. A wireless sensor network of such magnitude is unprecedented, and perceptive computer systems will extend to every corner of the globe. Information can be generated and shared locally in a peer-to-peer manner without the need for restrictive infrastructure.

The capabilities of future vehicles open up a number of potential applications for use in daily life. The main applications of VANET can be categorized as:

- ***Safety applications*:** pre-collision warning, electronic road signs, traffic light violation warning, online vehicle diagnosis, and road condition detection. This type of application usually takes advantage of short-range communication to perform real-time detection and provide warnings to drivers.

- ***Efficiency applications*****:** municipal traffic management, traffic congestion detection, route planning, highway tolling, and public transportation management. This type of application is dedicated to improving both individual and public travel efficiency.
- ***Commercial applications*****:** Location-Based Services (LBS) will give rise to a variety of commercial applications such as nearby restaurant specials, cheap gas stations, or even shopping center promotions. Such commercial applications may spur new competition among local businesses.
- ***Infotainment applications*****:** video and music sharing, location-based restaurant or store reviews, carpooling, and social networking. Already, infotainment applications such as Ford Sync and Kia UVO have become attractive add-ons in the vehicle market. The networking of infotainment systems will surely be a trend soon.

An abundance of VANET applications will benefit a wide range of parties: from governments and vehicle manufacturers to local retailers and consumers. Although a few Geographic Information Systems (GIS) companies—such as Google, Garmin, and TomTom—have engaged in collecting and distributing traffic information, traditionally, ITS development and deployment has been the domain of governments. In the future, many more participants will be attracted to VANET and will profit from it. Vehicle manufacturers could predict a boost in their sales by selling VANET-enabled vehicles. Fitting vehicles with a variety of electronic controls and devices is a growing trend, especially fitting electronic safety and information systems. Ford Sync is a very successful example of vehicle infotainment. Moreover, local retailers and service providers will also be interested in promoting their sales via VANET. They could broadcast commercials to passing vehicles and even devise hourly pricing strategies. Local businesses may gain a competitive advantage or face greater competition. Undoubtedly, consumers will be the beneficiary of enhanced safety and efficiency, cheaper goods, enriched entertainment, and other advantages.

A) Inter-vehicle communication

The inter-vehicle communication configuration (Fig. 5.2) uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: *naïve broadcasting* and *intelligent broadcasting*. In *naïve broadcasting*, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The limitations of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times. *Intelligent broadcasting* with implicit acknowledgement addresses the problems inherent in naïve broadcasting by limiting the number of messages broadcast for a given emergency event. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

B) Vehicle-to-roadside communication

The vehicle-to-roadside communication configuration (Fig. 5.3) represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle violates the desired speed limit, a broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting that the driver reduce his speed.

C) Routing-based communication

The routing-based communication configuration (Fig. 5.4) is a multi-hop unicast where a message is propagated in a multi- hop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

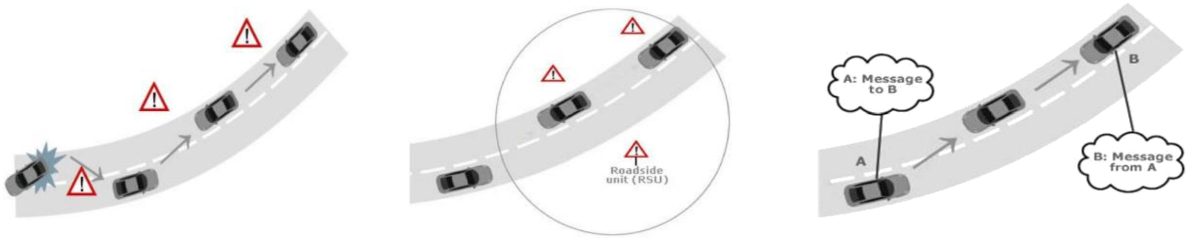
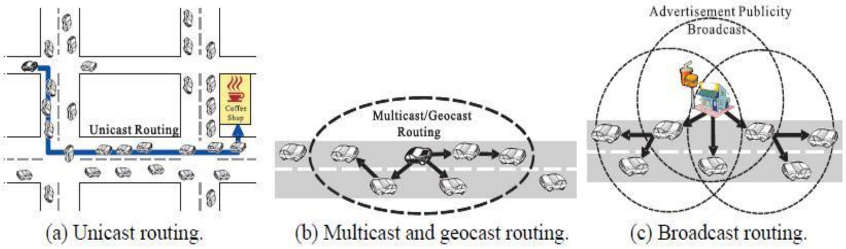


Figure 4

A) Inter-vehicle communication. B) Vehicle-to-roadside communication. C) Routing-based communication.

ROUTING

Routing in VANET has been studied and investigated widely in the past few years. Since VANETs are a specific class of ad hoc networks, the commonly used ad hoc routing protocols initially implemented for MANETs have been tested and evaluated for use in a VANET environment. Use of these address-based and topology-based routing protocols requires that each of the participating nodes be assigned a unique address [25]. This implies that we need a mechanism that can be used to assign unique addresses to vehicles but these protocols do not guarantee the avoidance of allocation of duplicate addresses in the network. Thus, existing distributed addressing algorithms used in mobile ad-hoc networks are much less suitable in a VANET environment. Specific VANET-related issues such as network topology, mobility patterns, demographics, density of vehicles at different times of the day, rapid changes in vehicles arriving and leaving the VANET and the fact that the width of the road is often smaller than the transmission range all make the use of these conventional ad hoc routing protocols inadequate.



(a) Unicast routing. (b) Multicast and geocast routing. (c) Broadcast routing.

Figure 5: Application for VANET.

The growth of the increased number of vehicles are equipped with wireless transceivers to communicate with other vehicles to form a special class of wireless networks, known as vehicular ad hoc networks or VANETs . To enhance the safety of drivers and provide the comfortable driving environment, messages for different purposes need to be sent to vehicles through the inter-vehicle communications. *Unicast* routing is a fundamental operation for vehicle to construct a source-to-destination routing in a VANET as shown in Fig. 5.5(a). *Multicast* is defined by delivering multicast packets from a single source vehicle to all multicast members by multi-hop communication. *Geocast* routing is to deliver a geocast packet to a specific geographic region. Vehicles located in this specific geographic region should receive and forward the geocast packet; otherwise, the packet is dropped as shown in Fig. 5.5(b). *Broadcast* protocol is utilized for a source vehicle sends broadcast message to all other vehicles in the network as shown in Fig. 5.5(c). Many results on MANETs have been proposed for unicast, multicast and geocast, and broadcast protocols. However, VANETs are fundamentally different to MANETs, such as the special mobility pattern and rapid changed topology. This key differentiation causes the existing routing protocol on MANETs cannot be directly applied to VANETs. In this investigation, the recent new results for VANET routing mechanism are first surveyed. Fig. 5.6 shows that the survey is structured into three broad categories; unicast, multicast and geocast, and broadcast approaches. The key ideas of representative technologies in each category are described.

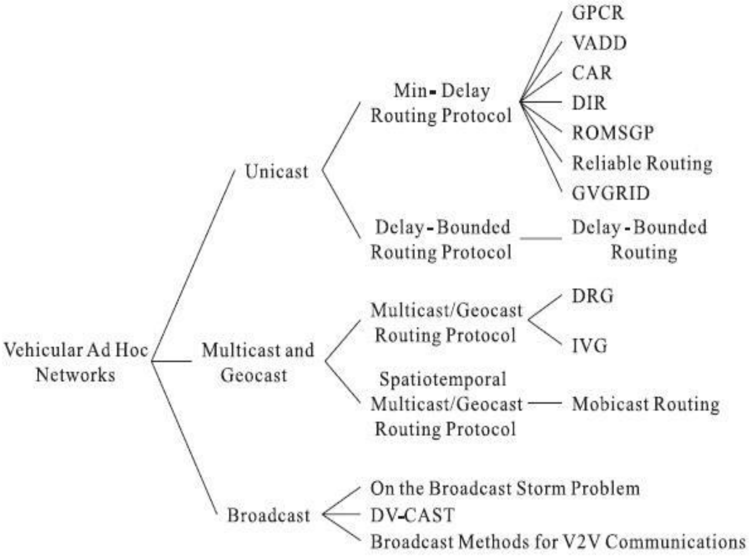

Vehicular Ad Hoc Networks
Unicast
Min- Delay Routing Protocol
GPCR
VADD
CAR
DIR
ROMSGP
Reliable Routing
GVGRID
Delay-Bounded Routing Protocol
Delay-Bounded Routing
Multicast and Geocast
Multicast/Geocast Routing Protocol
DRG
IVG
Spatiotemporal Multicast/Geocast Routing Protocol
Mobicast Routing
Broadcast
On the Broadcast Storm Problem
DV-CAST
Broadcast Methods for V2V Communications

Figure 6: The taxonomy of vehicular ad hoc networks.

OPPORTUNISTIC NETWORK (OPPNET)

The literal meaning of the term ‘opportunistic‘ is evident the tendency of network devices to exploit available resources in the network as and when possible. In the context of communication networks, though, it represents many more subtle properties [21]. Opportunistic networks are intrinsically fault tolerant for they are not limited by the end-to-end connectivity assumption. These networks are distributed and self-organizing in that the control and management is largely up to the individual devices or users (within the boundaries defined by the network operator‘s policies, if part of a commercial network). The communication in these networks is localized, i.e., decisions such as routing are made by devices based on locally available information. Opportunistic also means being able to take advantage of locally accessed global information, where devices implicitly convey global reach ability information strictly through local interaction. This type of network are useful in condition of disaster where network or communication line which we are currently using shuts down and people can help each other to communicate. Though there are some issues with reliability and security of opportunistic network as for reliability packet will be forward in the direction opposite to which destination node is wasting bandwidth. Security in opportunistic network is a biggest problem as packets will pass from many nodes between source and destination there is no guarantee that security will be preserved.

The woman at the desktop opportunistically transfers, via a Wi-Fi link, a message for a friend to a bus crossing the area, hoping that the bus will carry the information closer to the destination. The bus moves through the traffic, then uses its Bluetooth radio to forward the message to the mobile phone of a girl that is getting off at one of the bus stops. The girl walks through a near park to reach the university. Her cellular phone sends the message to a cyclist passing by. By proceeding in the same way some hops further, the message eventually arrives at the receiver. As it is clearly shown in this example, a network connection between the two women never exists but, by opportunistically exploiting contacts among heterogeneous devices, the message is delivered hop-by-hop (hopefully) closer to the destination, and eventually to the destination itself.

Wireless network infrastructures have been expanding at a rapid pace throughout the world. However, wireless networks may still not be available in areas such as poor regions, underwater sensors, or military operations. In order to provide networking support for situations where there are no directly connectivity paths, opportunistic network can be applied. Opportunistic network is a type of delay tolerant, intermittently connected network using an ad-hoc like structure. When a node wants to deliver data to another node but there does not exists a direct connection between them, packets can be forwarded to intermediate participating nodes which aid in delivering the packet from the source to the destination. Unlike a typical ad-hoc structure, however, opportunistic network assumes there is almost never a fully connected path between source to destination and the intermediate nodes may not encounter other nodes frequently or consistently. In some cases, intermediate nodes may have to buffer the packets received for a long time. Due to the uncertainty of packet delivery success in opportunistic networks, numerous routing protocols were proposed to maximize packet delivery rate. One of the most well-known routing protocols for opportunistic networks is a protocol called PRoPHET [3]. Since the chance of having a directly connected path from a source node to the destination node is rare or non-existent, identifying potential follow. Intermediate carriers for the packets to be transferred are essential. Forwarding data to intermediate carriers that rarely encounter the destination node will, in the worst case, fail to deliver the data. PRoPHET uses a predictability value, which is calculated using the history of encounters between nodes to evaluate the packet forwarding preference. While PRoPHET has shown decent results, there is still room for improvements. Due to the FIFO queuing nature of PRoPHET, packets may be dropped consistently when packets are forwarded to a few concentrated nodes. Packets may also be lost due to node failures or incomplete transmissions [5]. And another protocol is Epidemic routing [4] in which a node A ‖infects‖ every contact B with packets that it has that B doesn‘t have. A summary vector is typically exchanged to determine the missing packets. Epidemic routing is unbeatable from the point of view of successful delivery as long as the load does not stress the resources (bandwidth, storage).

The main ideas of the security solutions are providing secured transmission of the messages. Based on this consumption we need to efficiently protect the data forwarding mechanisms. First of all, we need to identify the potential attacker. We can classify the potential attacker into two groups:

- ***Internal attacker–*** it is a participant on routing and dissemination process. This kind of attacker can be selfish and malicious. Selfish attacker performs an attack only if directly participates on routing or dissemination. A malicious node can be viewed as a who simply cause damage to the network
- ***External attacker*** – have the limited permission to access to the OppNets.

ADVANTAGES AND USAGE OF OPPORTUNISTIC NETWORKS

According to the description above, an opportunistic network is not reliable if you want to send data to a specific node. Also it is impossible to maintain a stable connection between nodes. Although opportunistic networks are not reliable for data transmission, they are still very useful for many applications.

With the development of technology, wireless technologies such as Bluetooth, Wi-Fi, and so on are equipped in various mobile devices (mobile phone, PDA, mp3 player, etc.) which has increased the use of wireless ad hoc network applications. These applications are widely used for building sensor networks, data sharing, Internet collaborating etc. [4]. However, in a realistic environment, the traditional communication model of mobile ad hoc networks (MANET) which requires at least one path existing from the data source to target node is not able to build a structured and fully connected network. So for much of the time the whole network is disconnected for reasons which include signal attenuation, link loss, low density, node movement. As a result, communication failure is increased. Opportunistic networks which do not require a full network connection can solve the problems for many application fields. In an opportunistic network, communication opportunities arise from node movement to forward messages in a node-by-node way. The whole message forwarding process does not require a fully connected network. As the needs of self-organized networks increase so rapidly, many researchers have shown their interest in opportunistic networks. Although opportunistic networks are still in the developing step, some applications have already been set up. The following lists some typical applications of opportunistic networks:

- Wild animal tracing
- Handheld devices network organizing or mobile networking
- Car networks
- Network transmission in remote regions.

SIMULATION & RESULT

Simulation Setup

To study and evaluate the performance of the ProEp protocol, I have developed the wireless network Simulator framework. The simulator contains a model of the wireless nodes. Furthermore, the simulator has the limited number of nodes. Nodes are moving within the bounded area randomly with a varying speed. To aid in the evaluation of the protocol, I have develop a simple simulator. The simulator focuses on the operation of the routing protocols, and does not simulate the details of the underlying layers. When doing an evaluation of a protocol or system, it is very important that the models used in the evaluation are realistic. Since I base our protocol on making predictions depending on the movements of nodes, it is vital that the mobility models I use are realistic. One mobility model that has been commonly used in evaluations of ad hoc routing protocols is the random way-point mobility model. In this model, nodes randomly choose a destination and a speed and move there. Upon arrival at the destination, the nodes pause for a while and then choose a new destination.

In this evolution of the given protocol, I have focused on comparing the performance with regard to the following metrics. First, I am interested in the *message delivery delay*, i.e. to find out how long time it takes a message to be delivered. Even though applications using this kind of communication should be relatively delay-tolerant, it is still of interest to consider the change the *hope count* and *queue size* values. This indicates how the system resource utilization is affected by the different settings, which is crucial so that valuable resources such as bandwidth and energy are not wasted.

I ran simulations for each scenario several times, varying the queue size at the nodes (the number of messages can buffer) and the hop count value set in the messages. Following values for parameters are kept fixed in our simulation.

Parameter	**Values**
^{P}init	0.75
γ	0.25
B	0.98

Figure 7: Parameter Setting

The setup of experiment includes 24 nodes on approximately 100m X 100m. I am taking nodes with varying hop count & queue size. Nodes ranges from 16 to 24 with the hop count value 3 & 5 and queue size with 5 and 10 number of message storing capacities.

RESULTS

The performance could be measured using the following parameters:

1. Number of hop count given for the message.
2. Queue or buffer size of the node.
3. Travelling time (delay) of the message from source to the destination.
4. Number of nodes available on the field.
5. Speed of node

Result analysis using Travel time (delays)

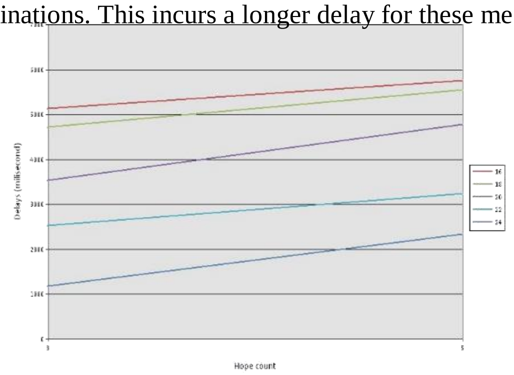
Initially I am taking different nodes separately and observe the effect with change in hop count and queue size value with all four combinations. In each case I plotted a graph with reference to delays (average travel time), as seen in Fig. 8.2 and 8.3.

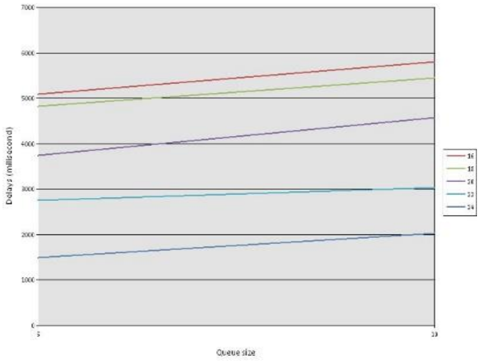
As seen in Fig. 8.2, decrease in the number of nodes the direct effect on the delays. When hop count is 3, the average travel time is lesser than hop count value 5. It is because if decrease in the hop count value, there will be less number of intermittent nodes. If message will reach to its hop count value message would be dropped. So when hop count value was less and tried to send message with such minimum value, if destination was not found within that hop count value, ultimately message was dropped. So it is better to have minimum value for hop count which ultimately goes through lesser number of intermittent nodes and requires less time to travel. But chosen low value for hop count this will leads to message drops when hop count value will reach. And increase in the value for hop count affects greater delays.

After that changing the values of queue size and then observe the changes which shown in Fig. 8.3. Now in this case increase in the size of queue, the delays would be increases. As we know, queue means the buffer which holds the message generated by self and received while moving around the network for routing purpose. So when increase in the buffer capacity so fewer messages would drop. But this will affect the message exchange capabilities, when more messages are in queue it can‘t drop more messages for new ones.

Fig. 8.2 and 8.4 have only one difference that, in Fig. 8.2, I am taking nodes separately but in Fig. 8.4, I consider average values for all nodes in observation. Fig. 8.4 clearly shows that increase in the value of hop count would results in higher delays. It is because as the intermittent nodes increases off course delays should increasers parallel.

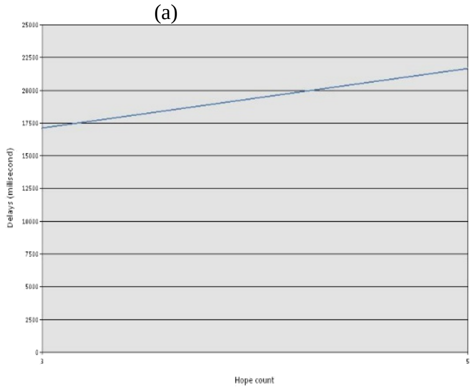
Similarly, Fig. 8.3 and 8.5 have only one difference that, in Fig. 8.3 I am taking nodes separately but in Fig. 8.5 I considering average values. Fig. 8.5 clearly shows that increase in the value of queue size would results in fewer delays.Effect of decreasing the number of nodes would result in similar results as hop count results. Here also decrease in nodes will have increases the delays because of less intermittent nodes for routing the messages. Looking at the delivery delay graphs Fig. 8.5, it seems like increasing the queue size, also increases the delay for messages. However, the phenomenon seen is probably not mainly that the delay increases for messages that would be delivered even at a smaller queue size (even though large buffers might lead to problems in being able to exchange all messages between two nodes, leading to a higher delay), but the main reason the average delay is higher is coupled to the fact that more messages are delivered. These extra delivered messages are messages that were dropped at smaller queue sizes, but now are able to reside in the queues long enough to be delivered to their destinations. This incurs a longer delay for these messages, increasing the average delay.

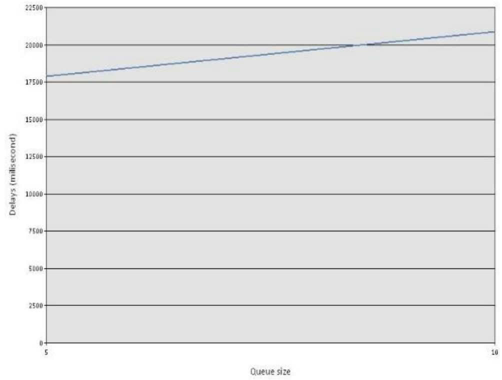




(a)

(b)





(8.2) Graph of Hope count vs. delay with different nodes
(8.3) Graph of Queue size vs. delay with different nodes
(8.4) Graph of Hope count vs. delay
(8.5) Graph of Queue size vs. delay

Parameter	**Value**
Total Simulation Time	5000 seconds
World Size	450 X 340 m
Movement Model	RandomWaypoint
Routing Protocol	PRoEp, Prophet, Epidemic
No of Nodes	5,10,20,30,40,50,100
Interface Transmit Speed	2 Mbps
Interface Transmit Range	100 m

msgTTL	300 min
Node Movement Speed	Min=0.5m/s Max=1.5m/s
Message creation rate	One message per 25-35 sec
Message Size	500 KB to 1MB

In the simulated environment, we have focused on comparing the performance with regard to the metrics defined above. The results presented here are obtained by running the simulations as per the parameters defined in Figure

A. Delivery Probability

From Fig. 8.9, it is evident that the delivery probability of ProEp routing protocol in the considered scenario is high as compared to the delivery probability of Epidemic and Prophet routing protocol. The delivery probability of Epidemic and Prophet routing protocol is almost same and lagging as the Number of nodes increased from 5 to 100

REFERENCES

I. M. Frodigh, P. Johansson, and P. Larsson. “Wireless ad hoc networking: the art of networking without a network,” Ericsson Review, No.4, 2000, pp. 248-263.

II. IETF Working Group: Mobile Adhoc Networks (manet). http://www.ietf.org/html.charters/manet-charter.html.

III. Ad Hoc Networking Extended Research Project. Online Project. http://triton.cc.gatech.edu/ubicomp/505.

IV. IEEE 802.11 Working Group. http://www.manta.ieee.org/groups/802/11/.

V. E.M. Royer and C.K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks,” IEEE Personal Communications, 1999, 6(2), pp. 46-55.

VI. S.R. Das, R. Castaneda, and J. Yan, “Simulation-based performance evaluation of routing protocols for mobile ad hoc networks,” Mobile Networks and Applications, 2000, 5, pp. 179-189.

VII. S.-J. Lee, M. Gerla, and C.-K. Toh, “A simulation study of table-driven and on-demand routing otocols for mobile ad-hoc networks,” IEEE Network, 1999, 13(4), pp. 48-54.

VIII. M. Joa-Ng and I.-T. Lu, “A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks,”. IEEE Journal on Selected Areas in Communications, 1999, 17(8), pp. 1415-1425.

IX. L. Ji, M. Ishibashi, and M.S. Corson, “An approach to mobile ad hoc network protocol kernel design,” In Proceedings of IEEE WCNC’99, New Orleans, LA, Sep. 1999, pp. 1303-1307.

X. Y.-B. Ko and N. H. Vaidya, “Geocasting in mobile ad hoc networks: Location-based multicast algorithms,”. Technical Report TR-98-018, Texas A&M University, Sep. 1998.

XI. M. Gerla, C.-C. Chiang, and L. Zhang, “Tree multicast strategies in mobile, multihop wireless networks,” ACM/Baltzer Mobile Networks and Applications, speical issue on Mobile Ad Hoc Networking, 1999, 4(3), pp. 193-207.

XII. S. Chakrabarti and A. Mishra, “QoS issues in ad hoc wireless networks,” IEEE Communications Magazine, 2001, 39(2), pp. 142–148.

XIII. L. Zhou and Z. J. Haas, “Securing ad hoc networks,” IEEE Network Journal, 1999, 13(6), pp. 24-30.

XIV. E. Pagnani and G. P. Rossi, “Providing reliable and fault tolerant broadcast delivery in mobile ad-hoc networks,” Mobile Networks and Applications, 1999, 5(4), pp. 175-192.