ISLAMIC UNIVERSITY OF TECHNOLOGY

STUDY ON VEHICULAR AD-HOC DELAY TOLERANT NETWORKING FOR INFRASTRUCTURE-LESS AREAS

Authors

Md. Saniad (102402)

S.M.A. Sayem (102404)

Abrar Zahin (102462)

Supervisor

Khondokar Habibul Kabir, Ph.D.

Assistant Professor,

Department of Electrical and Electronic Engineering

A thesis submitted to the Department of EEE in partial fulfillment of the requirements for the degree of B.Sc. Engineering in EEE

Academic Year: 2013-2014

Declaration of Authorship

This is to certify that the work presented in this thesis is the outcome of the analysis and investigation carried out by Md. Saniad, S. M. A. Sayem and Abrar Zahin under the supervision of Dr. Khondokar Habibul Kabir in the Department of Electrical and Electronic Engineering (EEE), Islamic University of Technology, Gazipur, Bangladesh. It is also declared that neither of the thesis nor any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Authors:

_____

Md. Saniad

Student ID: 102402

_____

S. M. A. Sayem

Student ID: 102404

_____

Abrar Zahin

Student ID: 102462

A Dissertation on,

"Study on Vehicular Ad-Hoc Delay Tolerant Networking for Infrastructure-less Areas"

Approved By

_____

Prof. Dr. Md. Shahid Ullah
Head of the Department & Professor
Department of EEE, IUT

Supervised by

_____

Dr. Khondokar Habibul Kabir
Thesis Supervisor & Assistant Professor
Department of EEE, IUT

ABSTRACT

Generally in traditional networks suppose the existence of some path between endpoints. Today, however, new applications, environments and types of devices are challenging these assumptions. In Delay Tolerant Networks (DTNs), an end-to-end path from source to destination may not exist. Nodes may connect and exchange their information in an opportunistic way. This book represents a broad overview of DTNs, particularly focusing on Vehicular Ad-hoc DTNs, their main characteristics, challenges and our research on this field. In the near future, cars are expected to be equipped with devices that will allow them to communicate wirelessly i.e. Wi-Fi. However, there will be strict restrictions to the duration of their connections with other vehicles, whereas the conditions of their links will greatly vary; DTNs as well as Ad-hoc DTNs present an attractive solution. Therefore, Vehicular Ad-hoc DTNs constitute an attractive research field. For practical implementation, we have used two Android devices for a little ranges of Wi-Fi. So by this we are trying to give us better accuracy to go further. Thorough out this document, we have mentioned those techniques we came across and also those techniques and algorithms that we used in our proposed method.

TABLE OF CONTENTS

1. Introduction..... 7

2. Delay Tolerant Network..... 8
   2.1. What is DTN? 8
   2.2. Beginning of Delay Tolerant Networking..... 8
   2.3. Why DTN? 9
   2.4. Generalization..... 10
   2.5. Aspects of DTN..... 11
   2.6. Contacts..... 13
      2.6.1. Persistent Contact..... 13
      2.6.2. Intermittent Scheduled Contact..... 13
      2.6.3. Intermittent Opportunistic Contacts..... 13
      2.6.4. Intermittent – Predicted Contact..... 13
   2.7. Applications of DTN..... 14
3. Ad-hoc Network..... 15
   3.1. Aspects of Ad-Hoc Network..... 16
   3.2. Ad Hoc Network Applications..... 18
   3.3. Indispensability Ad-hoc network..... 20
   3.4. Mobile Ad-Hoc Network (MANET)..... 21
      3.4.1. Internet Based MANET..... 21
   3.5. Vehicular Ad-Hoc Network (VANET)..... 22
      3.5.1. Background..... 23
      3.5.2. Data transmission by VANET..... 23
      3.5.3. Challenges and requirements in VANET Design..... 23
      3.5.4. Security Challenges in VANET..... 24
      3.5.5. Evaluation..... 25
      3.5.6. VANET Applications..... 26
      3.5.7. Factors affecting VANETs quality..... 26
4. Vehicular Ad-Hoc Delay Tolerant Network for infrastructure-less areas 27
   4.1. Model Scenario..... 27
   4.2. Data Delivery Schemes..... 30
      4.2.1. One Way One Direction..... 30
      4.2.2. Multi-Hop One Direction..... 32
      4.2.3. Multi-Hop Multi-Direction..... 33

4.3. Simulation..... 35
4.3.1. Simulation Setup..... 35
5. Results and Discussions..... 36
6. Conclusion & Future Plan..... 68

References..... 69

Chapter 1

Introduction

The existing Internet protocols do not work well for some environments, due to some fundamental assumptions built into the Internet architecture that an end-to-end path between source and destination exists for the duration of a communication session, end-to-end loss is relatively small, all routers and end stations support the TCP/IP protocols that applications need not worry about communication performance. But Delay Tolerant Network (DTN) architecture is conceived to relax most of these assumptions by using storage within the network to support store-and-forward operation over multiple paths and over potentially long timescales [11].Our motivation is to a create network to transfer data in infrastructure-less areas. Such scenario can be in highways where there is no fixed structure or tower to transfer data. Create network in such scenario, we can use Ad hoc Delay Tolerant Network where- we can use each vehicle, which can be regarded as mobile node. Each mobile node, i.e., vehicle are equipped with wireless networking devices, i.e., Wi-Fi device, smart phone. Information data must transfer in hop by hop manner from source to destination. We have tried to do it practically in a little scale. So that we can implement it in urban areas and if possible for rural areas in our country (Bangladesh). For that we are trying to develop our practical implementation segment. This is a great chance to connect people from the remote corner of the country.

Chapter 2

Delay Tolerant Network

2.1 What is DTN? :

Delay-tolerant networking (**DTN**) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet [16]. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. Recently, the term disruption-tolerant networking has gained currency in the United States due to support from DARPA, which has funded many DTN projects [1]. Disruption may occur because of the limits of wireless radio range, sparsely of mobile nodes, energy resources, attack, and noise.

2.2 Beginning of Delay Tolerant Networking:

Researchers began developing technology for routing between non-fixed locations of computers [1]. While the field of ad hoc routing was inactive throughout the 1980s, the widespread use of wireless protocols reinvigorated the field in the 1990s as mobile ad hoc networking (MANET) and vehicular ad hoc networking became areas of increasing interest. Actually it started in the end of 1970s, spurred by the decreasing size of computers. Concurrently with (but separate from) the MANET activities, DARPA had funded NASA, MITRE and others to develop a proposal for the Interplanetary Internet (IPN). In 2002, Kevin Fall started to adapt some of the ideas in the IPN design to terrestrial networks and coined the term *delay-tolerant networking* and the DTN acronym. A paper published in 2003 SIGCOMM conference gives the motivation for DTNs. The mid-2000s brought about increased interest in DTNs, including a growing number

of academic conferences on delay and disruption-tolerant networking, and growing interest in combining work from sensor networks and MANETs with the work on DTN.

2.3 Why DTN? :

Many evolving and potential communication environments do not conform to the Internet's underlying assumptions. These environments are characterized by:

- Intermittent Connectivity: The absence of an end-to-end path between source and destination is called network partitioning. In such cases, communication using the TCP/IP protocols does not work [3].
- Long or Variable Delay: In addition to intermittent connectivity, long propagation delays between nodes and variable queuing delays at nodes contribute to end-to-end path delays that can defeat Internet protocols and applications that rely on quick return of acknowledgements or data [16].
- Asymmetric Data Rates: The Internet supports moderate asymmetries of bidirectional data rate for users with cable TV or asymmetric DSL service. But if asymmetries are large, they defeat conversational protocols.
- High Error Rates: Bit errors on links require correction (which requires more bits and more processing) or retransmission of the entire packet (which results in more network traffic). For a given link-error rate, fewer retransmissions are needed for hop-by-hop retransmission than for Internet-type end-to-end retransmission (linear increase vs. exponential increase, per hop).
- Intermittent connectivity: A growing number of communicating devices are in motion and operate on limited power. This is true in interplanetary space and is becoming more common on Earth among mobile wireless communication devices, such as cell phones. When communicating nodes are in motion, links can be obstructed by intervening bodies. When nodes must conserve power or preserve secrecy, links are shut down. These events cause intermittent connectivity [16]. When no path exists to connect a source with a destination, a network partition is said to occur.

2.4 Generalization:

DTNs overcome the problems associated with intermittent connectivity, long or variable delay, asymmetric data rates, and high error rates by using store-and forward message switching. This is a very old method, used by pony-express and postal systems since ancient times. Whole messages (entire blocks of application-program user data)—or pieces (fragments) of such messages—are moved (forwarded) from a storage place on one node (switch intersection) to a storage place on another node, along a path that eventually reaches the destination.

Utilizing the DTN approach requires significant effort developing additional functionality and integrating them. Delay-Disruption Tolerant networks make use of "Store – and – Forward", mentioned in Fig 2.1 below, technique within the network in order to compensate Intermittent Link Connectivity. Store-and-forwarding methods are also used in today's voicemail and email systems, but these systems are not node-to-node (like below figure 2.1, node X,Y,Z,W) relays (as shown above) but rather star relays; both the source and destination independently contact a central storage device at the center of the links [16].

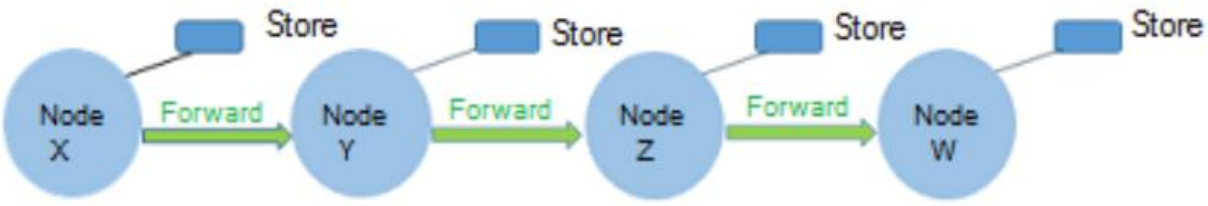


Fig 2.1: Store and Forward Technique

In the DTN, the fundamental concept is an Architecture based on Internet – Independent Middleware, where the protocols at all layers are used that bets suite the operation within each environment, with a new overlay network called Bundle Protocol (BP) inserted between application & the locally optimized communication stacks. Military applications in the DTN areas are substantial, allowing the retrieval of critical information in mobile battlefield scenarios using only intermittently connected network communications. For these kinds of applications, the DTN protocol should transmit data segments across multi – hop networks that

consists of different regional networks based on environmental network parameters. In all the cases, the operation requirements are differently altered and their performance is negatively altered rendering them Heterogeneous nature.

DTN routers need persistent storage for their queues for one or more of the following reasons:

- A communication link to the next hop may not be available for a long time.
- One node in a communicating pair may send or receive data much faster or more reliably than the other node.
- A message, once transmitted, may need to be retransmitted if an error occurs at an upstream (toward the destination) node, or if an upstream node declines acceptance of a forwarded message [16].

The network uses variety of communication nodes, such as wireless, satellites, vehicle-mounted and unmanned aerial vehicle, to continuously advance message traffic even when there's an obstacle in the path that would stop traffic in the traditionally network. The delay tolerant networks makes the network to continue its function reliably in the environment where communications are most challenging and most critical and the message traffic continues to flow despite geographical or structural or malicious disruptions. The DTN Architecture is designed to effectively operate as an overlay on top of regional networks or as an Inter Planetary internet. Moreover, the Delay Tolerant Network can overcome problems characterized by Long – Delays, Asymmetric Data Rates, Intermittent Connectivity, High Error Rates due to extreme environments, distances encountered in Space communication at Inter–Planetary scale competently when compared with the traditional Internet suite.

2.5 Aspects of DTN:

When the link is up, the source node has an opportunity to send the data to other end. In DTN, this opportunity is called "Contact". More than one contact may be available between a given pair of nodes. For example: a node might have both high-Performance, expensive connections and a Low-Performance cheap connection simultaneously for communication with the same

direction. The "Contact Schedule" is the set of times when the Contact will be available, (i.e.) upon considering the Contact's in Graph Theory, it is a Time-Varying Multi-Graph. The DTN architecture proposes to use this network by forwarding the complete Data/Message over each hop. These Messages/Data will be buffered at each intermediate node, potentially on Non-Volatile Storage. This enable messages to wait until the Next-Hop is available; which may be a long period of time [4].

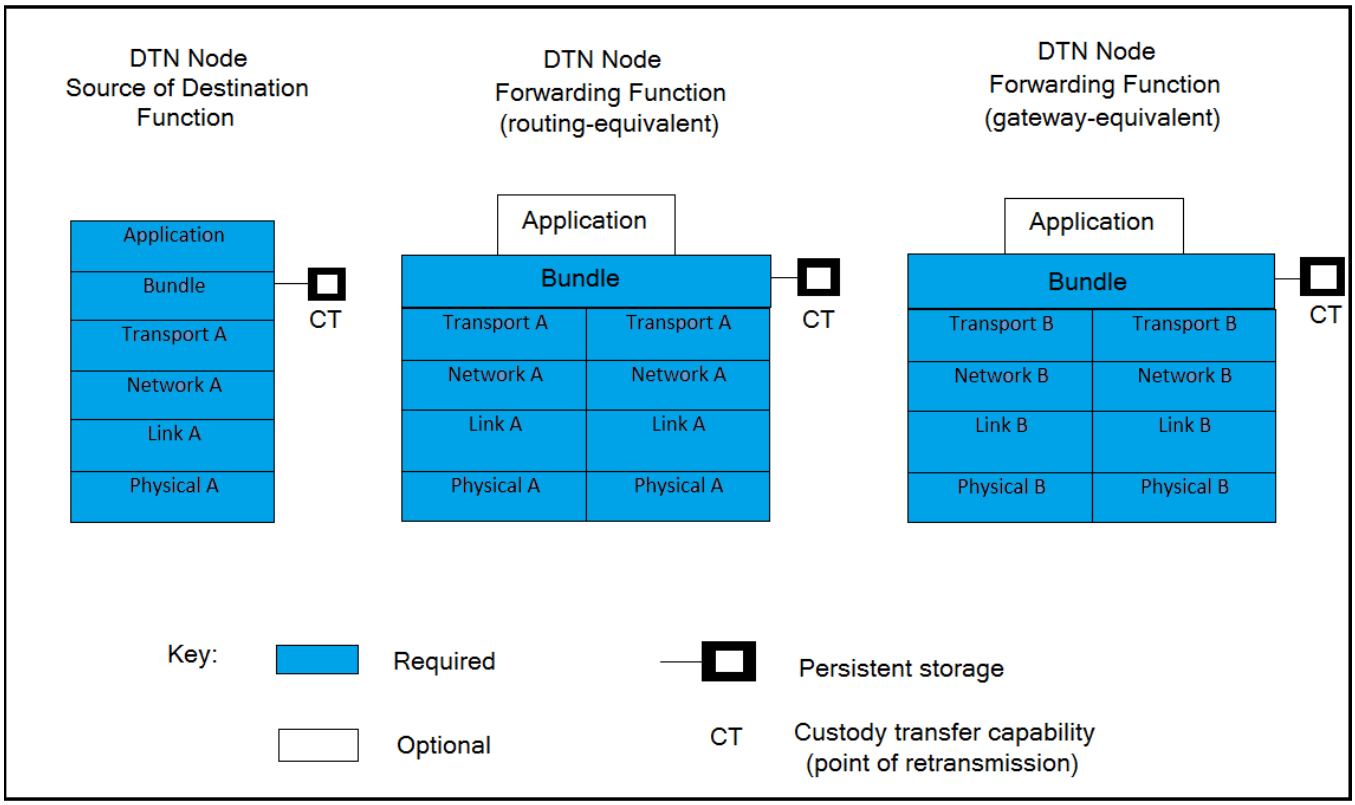


Fig 2.2: DTN node

In above figure 2.2, we can see the structure. Unlike the TCP/IP, the DTN does not assume a continuous end – to – end connection. In its design, if a destination path is un-reachable, the data packets are not discarded but instead each network node keeps custody of the data as long as necessary until it can positively communicate with other node which ensures that the information does not get lost when no intermediate path to the destination exists [16]. The DTN acts as an overlay above Transport Layers of the networks it interconnects and provides key services such as in-network data storage and retransmission, interoperable naming, authenticated forwarding and a coarse-grained class of service. TCP/IP suite functions

poorly when faced with very long delay paths and frequent network partition. These problems are aggravated by the end nodes that have Severe Power constraints or Memory constraints.

2.6 Contacts:

Contact and their volumes are known ahead of time, intelligent routing and forwarding decisions can be made (optimally for small networks. The Contacts in the Delay Tolerant Networks typically fall into one of several categories, based largely on the predictability of their performance characteristics & whether some action is required to bring them into existence. The following are the major types of contacts:

2.6.1 Persistent Contact:

Persistent Contacts are always available (i.e.) no connection initiation is required to instantiate a Persistent Contact. An 'always-on' Internet connection such as DSL (or) Cable Modem Connection is a representative of this class.

2.6.2 Intermittent-Scheduled Contact:

Scheduled contacts may involve message-sending between nodes that are not in direct contact, as shown in the figure below. They may also involve storing information until it can be forwarded, or until the receiving application can catch up with the sender's data rate.

2.6.3 Intermittent – Opportunistic Contacts:

Network nodes may need to communicate during opportunistic contacts, in which a sender and receiver make contact at an unscheduled time. Moving people, vehicles, aircraft, or satellites may make contact and exchange information when they happen to be within line-of-sight and close enough to communicate using their available (often limited) power.

This same model can apply to electronic communication. For example, wireless mobile devices such as cell phones can be designed to send or receive information when certain people carrying the mobile device come within communication range.

2.6.4 Intermittent – Predicted Contact:

Predicted Contacts are based on no fixed schedule, but rather are predictions of likely contact times and durations based on a history of previously observed contacts or some other information. This is an active research area [4].

2.7 Applications of DTN:

Although DTNs were originally conceived for interplanetary use, they may have a far greater number of applications on Earth. Here is a short summary of the possible applications [18]:

- Space Agencies: International Space Station communication (currently operational for research), interplanetary communication, future space-debris monitoring.
- Military and Intelligence: Mobile ad-hoc networks (MANETs) for wireless communication and monitoring, cargo tracking, search and rescue communication, unmanned aerial vehicle (UAV) communication and control.
- Commercial: Cargo and vehicle tracking (by road, rail, sea, and air), in-store and in-warehouse asset tracking, data transactions (e.g., financial, reservations), agricultural crop monitoring, processing-plant monitoring, communication in underground mines.
- Public Service and Safety: Security and disaster communication, search and rescue communication, humanitarian relief monitoring, smart-city event-response, smart transportation networks, smart electric-power networks, global airport-traffic control, infrastructure-integrity monitoring, unmanned aerial vehicle (UAV) communication and control, remote learning [5].
- Personal Use: Personal monitoring and communication in wilderness and urban areas, fire-and-forget text messaging. Environmental Monitoring: Animal migration, soil properties and stability, atmospheric and oceanographic conditions, seismological events.
- Engineering and Scientific Research: Network subject-matter experts, academic research by faculty and students.

Chapter 3

Ad-Hoc Network

Ad-hoc is a Latin word that means "for this purpose". A wireless **ad-hoc network** is a decentralized type of wireless network. 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, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

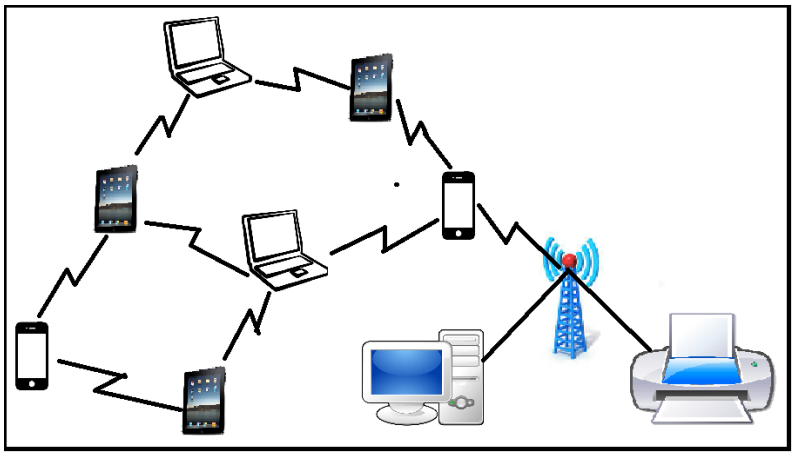


Fig 3.1: Ad-Hoc Network

An ad hoc network typically refers to any set of networks where all devices have equal status on a network, in above figure 3.1, we can see that and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of wireless networks.

The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly.

3.1 Aspects of Ad-Hoc Network:

Mobility: The nodes can be rapidly repositioned and/or move in ad-hoc networks. Rapid deployment in areas with no infrastructure often implies that the users must explore an area and perhaps form teams/swarms that in turn coordinate among themselves to create a taskforce or a mission. We can have individual random mobility, group mobility, motion along preplanned routes, etc. The mobility model can have major impact on the selection of a routing scheme and can thus influence performance.

Multi-hopping: A multi hop network is a network where the path from source to destination traverses several other nodes. Ad hoc nets often exhibit multiple hops for obstacle negotiation, spectrum reuse, and energy conservation. Battle-field covert operations also favor a sequence of short hops to reduce detection by the enemy.

Self-organization: The ad hoc network must autonomously determine its own configuration parameters including: addressing, routing, clustering, position identification, power control, etc. In some cases, special nodes (e.g., mobile backbone nodes) can coordinate their motion and dynamically distribute in the geographic area to provide coverage of disconnected islands

Energy conservation: Most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply and no capability to generate their own power (e.g., solar panels). Energy efficient protocol design (e.g., MAC, routing, resource discovery, etc.) is critical for longevity of the mission.

Scalability: In some applications (e.g., large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc.) the ad hoc network can grow to several thousand nodes. For wireless "infrastructure" networks scalability is simply handled by a hierarchical construction. The limited mobility of infrastructure networks can also be easily handled using Mobile IP or local handoff techniques. In contrast, because of the more extensive mobility and the lack of fixed references, pure ad hoc networks do not tolerate mobile IP or a fixed hierarchy structure. Thus, mobility, jointly with large scale is one of the most critical challenges in ad hoc design.

Security: the challenges of wireless security are well known - ability of the intruders to eavesdrop and jam/spoof the channel. A lot of the work done in general wireless infrastructure networks extends to the ad hoc domain. The ad hoc networks, however, are even more vulnerable to attacks than the infrastructure counterparts. Both active and passive attacks are possible. An active attacker tends to disrupt operations (say, an impostor posing as a legitimate node intercepts control and data packets; reintroduces bogus control packets; damages the routing tables beyond repair; unleashes denial of service attacks, etc.). Due to the complexity of the ad hoc network protocols these active at-tacks are by far more difficult to detect/fold in ad hoc than infrastructure nets. Passive attacks are unique of ad hoc nets, and can be even more insidious than the active ones. The active attacker is eventually discovered and physically disabled/eliminated. The passive attacker is never discovered by the network. Like a "bug", it is placed in a sensor field or at a street corner. It monitors data and control traffic patterns and thus infers the motion of rescue teams in an urban environment, the redeployment of troops in the field or the evolution of a particular mission. This information is relayed back to the enemy headquarters via special communications channels (e.g., satellites or UAVs) with low energy and low probability of detection. Defense from passive attacks require powerful novel encryption techniques coupled with careful network protocol designs.

Unmanned, autonomous vehicles: some of the popular ad hoc network applications require unmanned, robotic components. All nodes in a generic network are of course capable of autonomous networking. When autonomous mobility is also added, there arise some very interesting opportunities for combined networking and motion. For example, Unmanned Airborne Vehicles (UAVs) can cooperate in maintaining a large ground ad hoc network interconnected in spite of physical obstacles, propagation channel irregularities and enemy jamming. Moreover, the UAVs can help meet tight performance constraints "on demand" by proper positioning and antenna beaming.

Connection to the Internet: as earlier discussed, there is merit in extending the infrastructure wireless networks opportunistically with ad hoc appendices. For instance, the reach of a domestic wireless LAN can be extended as needed (to the garage, the car parked in the street, the neighbor's home, etc.) with portable routers. These opportunistic extensions are becoming increasingly important and in fact are the most promising evolution pathway to commercial applications. The integration of ad hoc protocols with infrastructure standards is thus becoming a hot issue.

3.2 Ad Hoc Network Applications:

In the past, the notion of ad hoc networks was often associated with communication on combat fields and at the site of a disaster area; now, as novel technologies such as Bluetooth materialize, the scenario of ad-hoc networking is likely to change, as is its importance.

Identifying the emerging commercial applications of the ad hoc network technology has always been an elusive proposition at best. Of the three wireless technologies - cellular telephony, wireless Internet and ad hoc networks - it is indeed the ad hoc network technology that has been the slowest to materialize, at least in the commercial domain. This is quite surprising since the concept of ad hoc wireless networking was born in the early 70's, just months after the successful deployment of the Arpanet, when the military discover the potential of wireless packet switching. Packet radio systems were deployed much earlier than any cellular and wireless LAN technology. The old folks may still remember that when Bob Metcalf (Xerox Park) came up with the Ethernet in 1976, the word spread that this was one ingenious way to demonstrate "packet radio" technology on a cable!

Application dependent nature of wireless ad-hoc networks is the motivation for examining a wide variety of system implementations in this tutorial. For example, WSNs have proven most suitable in situations where environmental monitoring is required across a spatially distributed area over an extended period of time. Thus examples from the military, agricultural, infrastructure and health monitoring predominate. Similar types of applications will be examined for each class of wireless ad-hoc network such as vehicular networks, multimedia networks,

delay tolerant networks, etc. In summary, the primary objective with this tutorial is to reach out to researchers from a breadth of research communities to show them the advantages Wireless Ad-Hoc Network implementations can bring to their specific problems of interest.

In fact, until recently, the driving application was instant deployment in an unfriendly, remote infrastructure-less area. Battlefield, Mars explorations, disaster recovery etc. have been an ideal match for those features. Early DARPA packet radio scenarios were consistently featuring dismounted soldiers, tanks and ambulances. A recent extension of the battlefield is the homeland security scenario, where unmanned vehicles (UGVs and UAVs) are rapidly deployed in urban areas hostile to man, say, to establish communications before sending in the agents and medical emergency personnel.

Recently an important new concept has emerged which may help extend ad hoc networking to commercial applications, namely, the concept of opportunistic ad hoc networking. This new trend has been in part prompted by the popularity of wireless telephony and wireless LANs, and the recognition that these techniques have their limits. The ad hoc network is used "opportunistically" to extend a home or Campus network to areas not easily reached by the above; or, to tie together Internet islands when the infrastructure is cut into pieces - by natural forces or terrorists for examples).

Two emerging wireless network scenarios that will soon become part of our daily routines are vehicle communications in an urban environment, and Campus nomadic networking. These environments are ripe for benefiting from the technologies discussed in this report. Today, cars connect to the cellular system, mostly for telephony services.

In future battlefield operations, autonomous agents such as Unmanned Ground Vehicles (UGVs) and Unmanned Airborne Vehicles (UAVs) will be projected to the forefront for intelligence, surveillance, strike, enemy antiaircraft suppression, damage assessment, search and rescue and other tactical operations. The agents will be organized in clusters (teams) of small unmanned ground, sea and airborne vehicles in order to launch complex missions that comprise several such teams. Examples of missions include: coordinated aerial sweep of vast urban/suburban areas to track suspects; search and rescue operations in unfriendly areas (e.g., chemical spills, fires, etc.), exploration of remote planets, reconnaissance of enemy field in the battle theater, etc. In those applications, many different types of Unmanned Vehicles (UVs) will be required,

each equipped with different sensor, video reconnaissance, communications support and weapon functions. A UV team may be homogeneous (e.g., all sensor UVs) or heterogeneous (i.e., weapon carrying UVs intermixed with reconnaissance UVs etc.). Moreover, some teams may be airborne, other ground, sea and possibly underwater based [5]. As the mission evolves, teams are reconfigured and individual UVs move from one team to another to meet dynamically changing requirements. In fact, missions will be empowered with an increasing degree of autonomy. For instance, multiple UV teams collectively will determine the best way to sweep a mine field, or the best strategy to eliminate an air defense system. The successful, distributed management of the mission will require efficient, reliable, low latency communications within members of each team, across teams and to a manned command post. In particular, future naval missions at sea or shore will require effective and intelligent utilization of real-time information and sensory data to assess unpredictable situations, identify and track hostile targets, make rapid decisions, and robustly influence, control, and monitor various aspects of the theater of operation [13].

Littoral missions are expected to be highly dynamic and unpredictable. Communication interruption and delay are likely, and active deception and jamming are anticipated. In a complex and large scale system of unmanned agents, such as designed to handle a battlefield scenario, a terrorist attack situation or a nuclear disaster, there may be several missions going on simultaneously in the same theater. A particular mission is "embedded" in a much larger "system of systems".

3.3 Indispensability for Ad-hoc Network:

An ad hoc network is made up of multiple "nodes" connected by "links". Links are influenced by the node's resources (e.g., transmitter power, computing power and memory) and behavioral properties (e.g., reliability), as well as link properties (e.g. length-of-link and signal loss, interference and noise). Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust, and scalable [14].

The network must allow any two nodes to communicate by relaying the information via other nodes. A "path" is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths.

3.4 Mobile Ad-Hoc Network (MANET):

A **mobile ad hoc network** (**MANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". 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. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table) [19]. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

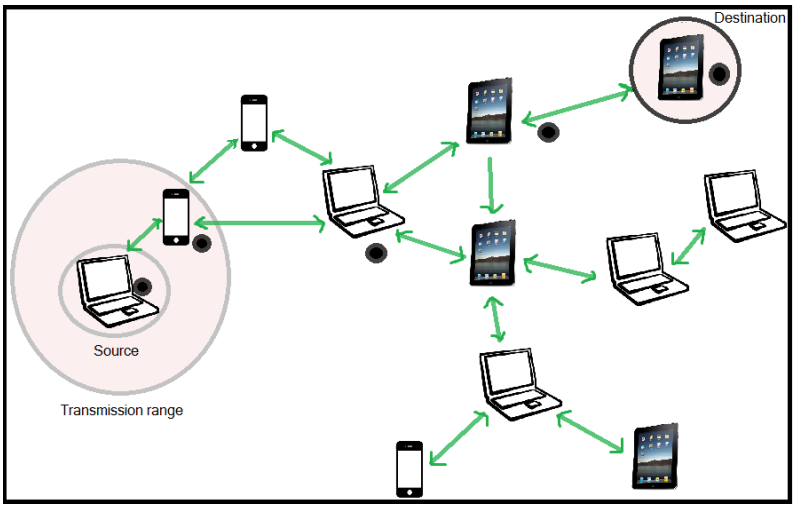


Fig 3.8: Mobile Ad-Hoc Network

In above figure 3.8, we can see MANET structure. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment [2]. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

3.4.1 Internet Based MANET:

Internet based mobile ad hoc networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad-hoc routing algorithms don't apply directly.

3.5 Vehicular Ad-Hoc Network (VANET):

Vehicular Ad hoc Networks (VANETs) belong to a subcategory of traditional Mobile Ad hoc Networks (MANETs). It is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 m of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

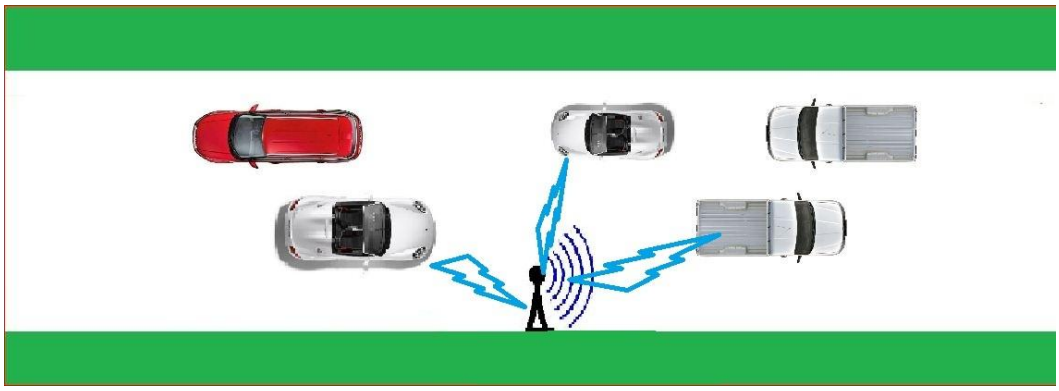


Fig 3.10: Vehicular Ad-Hoc Network (VANET)

In above figure 3.10, we can see the structure of VANET. Vehicular networks are fast emerging for developing and deploying new and traditional applications. More in detail, VANETs are characterized by high mobility, rapidly changing topology, and ephemeral, one-time interactions. Basically, both VANETs and MANETs are characterized by the movement and self-organization of the nodes (*i.e.*, vehicles in the case of VANETs). However, due to driver behavior, and high speeds, VANETs characteristics are fundamentally different from typical MANETs. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Our target is to transfer data between two sinks situated at the two ends of a highway.

3.5.1 Background:

VDTNs have evolved from DTNs and are formed by cars and any supporting fixed nodes. Fall (2003) is one of the first authors to define DTN and discuss its potential. According to his definition, a DTN consists of a sequence of time-dependent opportunistic contacts. During these contacts, messages are forwarded from their source towards their destination. One needs to find an effective route, both in time and space [20]. All nodes along the path should consider the nodes movement pattern and the possible communication opportunities for message forwarding. Unfortunately, it is not always easy to determine future communication opportunities or even forecast the mobility patterns of the nodes in the network.

3.5.2 Data transmission by VANET:

The main feature of VANETs is that mobile nodes are vehicles endowed with sophisticated "on-board" equipment's, traveling on constrained paths (*i.e.*, roads and lanes), and communicating each other for message exchange via Vehicle-to-Vehicle (V2V) communication protocols, as well as between vehicles and fixed road-side Access Points (*i.e.*, wireless and cellular network infrastructure), in case of Vehicle-to-Infrastructure (V2I) communications.

3.5.3 Requirements in VANET Design:

In the following we focus on two major issues in network layer design: security, and support of existing and future VANET applications. In the rest of this section we first discuss the common requirements of security in VANET and possible attacks to VANET. We then address the current and potential applications of VANET [13].

3.5.4 Security Challenges in VANET:

Some key issues are -High processing power and adequate power supply, known time and position, periodic maintenance and inspection, central registration, honest majority, existing law enforcement infrastructure

3.5.5 Evaluation:

To evaluate the routing algorithms for DTNs Jones (2006), and Sanchez, Franck & Beylot (2007), propose the utilization of [19]:

• Delivery ratio

• Latency: Even though the networks and applications are supposed to endure delays, many applications could take advantage of shorter delays. Even more, some application have time windows of delay resilience, i.e. messages are valid during a certain amount of time, after that the message loses its validity.

• Transmissions: The number of messages transmitted by the algorithms varies and some, that create multiple copies of the message, may send more messages than others.

• Lifetime: Route lifetime is the time a route can be used to forward packets without the need for re-computation.

• End-to-end delay: This evaluation criterion is the time it takes for one message to go from the origin to the destination.

• Capacity: Capacity is the amount of data that that may pass through one route during its lifetime

• Synchronicity: Even in a delay tolerant network, it is possible that, during some intervals, origin and destination are close and the communication may occur directly, or in the same way as it is in traditional wireless networks. Synchronicity, measures how long this situation where classical communication is possible.

• Simultaneousness: This criteria measures the contact durations. I.e. the time intermediate nodes are in the same area.

• Higher order simultaneousness

• Discontinuity: is the normalized duration of packet storage thorough the path.

3.5.6 VANET Applications:

It becomes a major challenge to support and enable diverse applications and services. Here we summarize the existing applications and several potential applications that have been proposed for VANET. It is important to note that we also elaborate on the functions of each application that shall be provided in the MAC layer and the network layer, so as to fulfill the requirements of these applications.

VANET would support life-critical safety applications, safety warning applications, electronic toll collections, Internet access, group communications, roadside service finder, etc. [12].

Life-Critical Safety Applications: Intersection Collision Warning/Avoidance, Cooperative Collision Warning, etc. In the MAC Layer, the Life-Critical Safety Applications can access the DSRC control channel and other channels with the highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Safety Warning Applications: Work Zone Warning, Transit Vehicle Signal Priority, etc. The differences between Life-Critical Safety Applications and Safety Warning Applications are the allowable latency requirements, while the Life-Critical Safety Applications usually require the messages to be delivered to the nearby nodes within 100 milliseconds, the Safety Warning Applications can afford up to 1000 milliseconds. The messages can be broadcasted to all the nearby VANET nodes.

Electronic Toll Collections (ETCs): Each vehicle can pay the toll electronically when it passes through a Toll Collection Point (a special RSU) without stopping. The Toll Collection Point will scan the Electrical License Plate at the OBU of the vehicle, and issue a receipt message to the vehicle, including the amount of the toll, the time and the location of the Toll Collection Point.

Internet Access: Future vehicles will be equipped with the capability so that the passages on the vehicles can connect to the Internet. In the MAC layer, the Internet Access

applications can use DSRC service channels except the control channel, with the lowest priority comparing with the previous applications. In the network layer, to support VANET Internet access, a straightforward method is to provide a unicast connection between the OBU of the vehicle and a RSU, which has the link toward the Internet.

Group Communications: Many drivers may share some common interests when they are on the same road to the same direction, so they can use the VANET Group Communications function. . In the past, Internet multicast has not been successful due to its complexity and, more important, because Internet multicast requires global deployment, which is virtually impossible. In a VANET, however, since all nodes are located in a relatively local area, implementing such group communication becomes possible [12].

Roadside Services Finder: Finding restaurants, gas stations, etc., in the nearby area along the road. A Roadside Services Database will be installed in the local area that connected to the corresponding RSUs. In the MAC layer, the Roadside Services Finder application can use DSRC service channels except the control channel, with the lowest priority comparing with the safety related applications and ETCs. Each vehicle can issue a Service Finder Request message that can be routed to the nearest RSU; and a Service Finder Response message that can be routed back to the vehicle [13].

3.5.7 Factors affecting VANETs quality:

Quality of service provided in a VANET is strongly affected by mobility of vehicles, and then dynamic changes of network topology. Different classes of vehicles can move in VANETs, depending on traffic conditions (*i.e.*, dense and sparse traffic), speed limits in particular roads (*i.e.*, highways, rural roads, urban neighborhoods), and also typology of vehicles (*i.e.*, trucks, cars, motorcycles, and bicycles). In general, compared to traditional mobile nodes in MANETs, vehicles in VANETs move at higher speeds (*i.e.*, from 0 to 40 m/s).

Chapter 4

STUDY ON VEHICULAR AD-HOC DELAY TOLERANT NETWORKING FOR INFRASTRUCTURE-LESS AREAS

4.1 Model Scenario:

We considered a highway where vehicles are moving. We wanted to send some data from one end to the other end. But if there is no end to end connection between the two ends, it is not possible to do this. That's why we build a Vehicular Ad-Hoc Delay Tolerant Network. In this case, each vehicle (truck or car) works as an individual node and router having a Wi-Fi device with Wi-Fi range and storage system. Whenever the Wi-Fi range of two cars/trucks overlap, they connect each other creating an Ad-Hoc Network .The sinks at two ends can simultaneously generate and receive data. The generated data by sink 1 or sink 2 is delivered to sink 2 or sink 1 respectively by the cars.

The basic algorithm to delivery data was –"**store and carry**". Every vehicle collected data from the sink and stored it. Then it carried the data by itself and whenever it found any other vehicle within its Wi-Fi range, it forwarded the collected data. Thus data delivery was done from one end to the other end. We needed some parameters, those are-

Sink: There were two sinks at two ends, sink 1 and sink 2. Each sink could generate and receive data simultaneously and the generated data was delivered by the vehicles.

Road: We considered the road consisting of two lanes. For our model we also considered a portion of the highway with a length of 5 km. We took the lanes ideal where there was no bending and there was no section or sub-section.

Vehicle: We took car and truck as vehicles. Car and truck could move in opposite direction. We assumed that, every vehicle had a data storage system and a power supply that supplies power.

Vehicles would always try to connect to each other within their Wi-Fi range. If a vehicle found any other vehicle within its range, it would deliver the data. The new vehicle then carried the data until it found another vehicle within its range. Thus data was stored, carried and forwarded to the sink. We also assumed that the vehicles would not change their route.

Wi-Fi range: Wi-Fi range of each vehicle was 250 m. Within this range a vehicle could connect with other vehicles and transfer data.

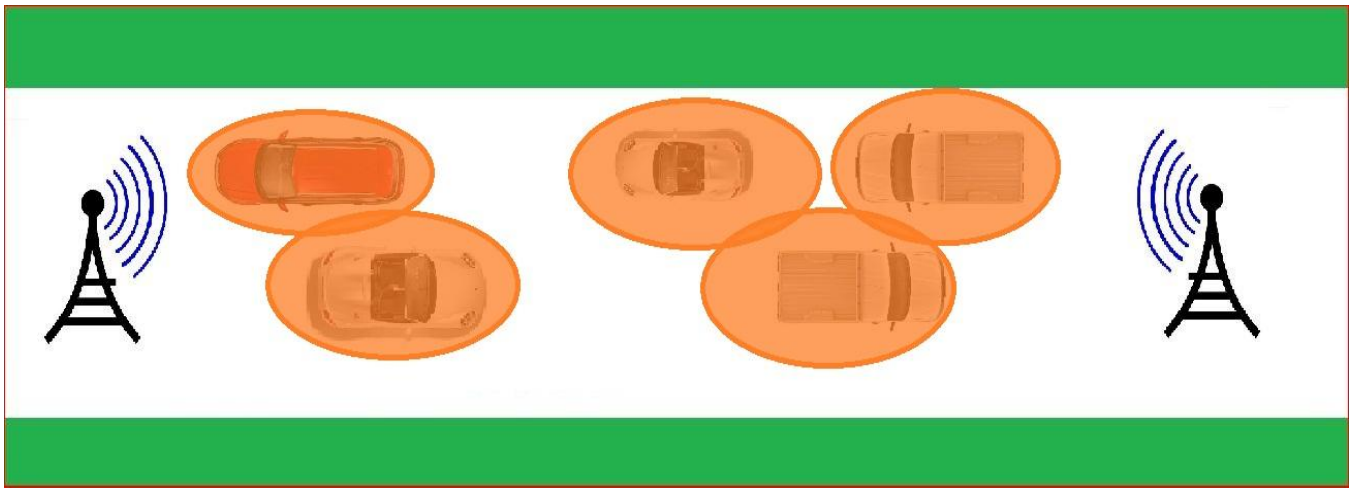
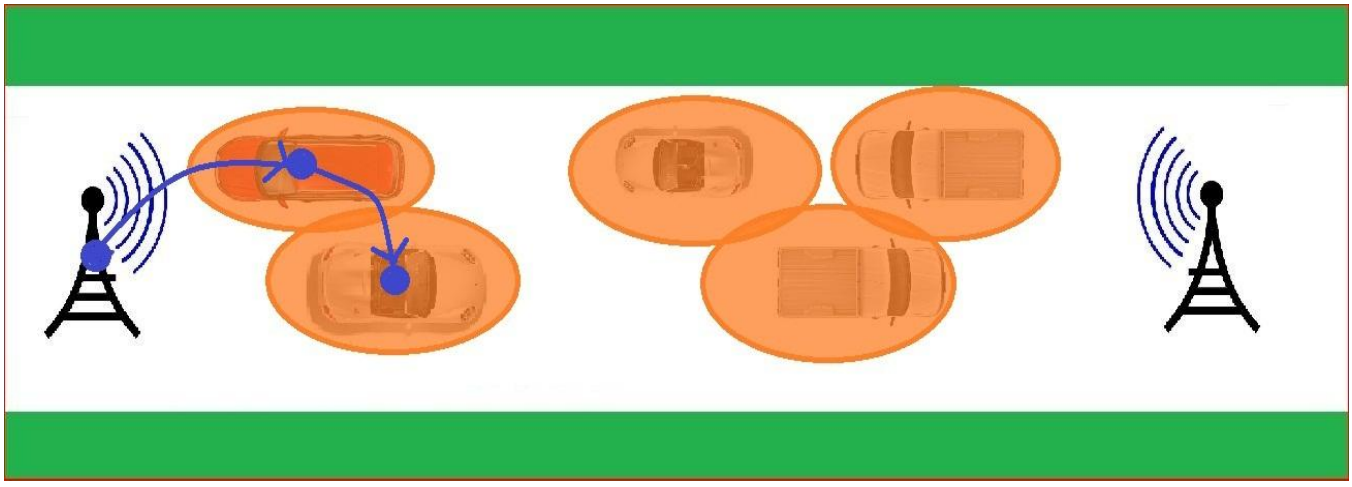
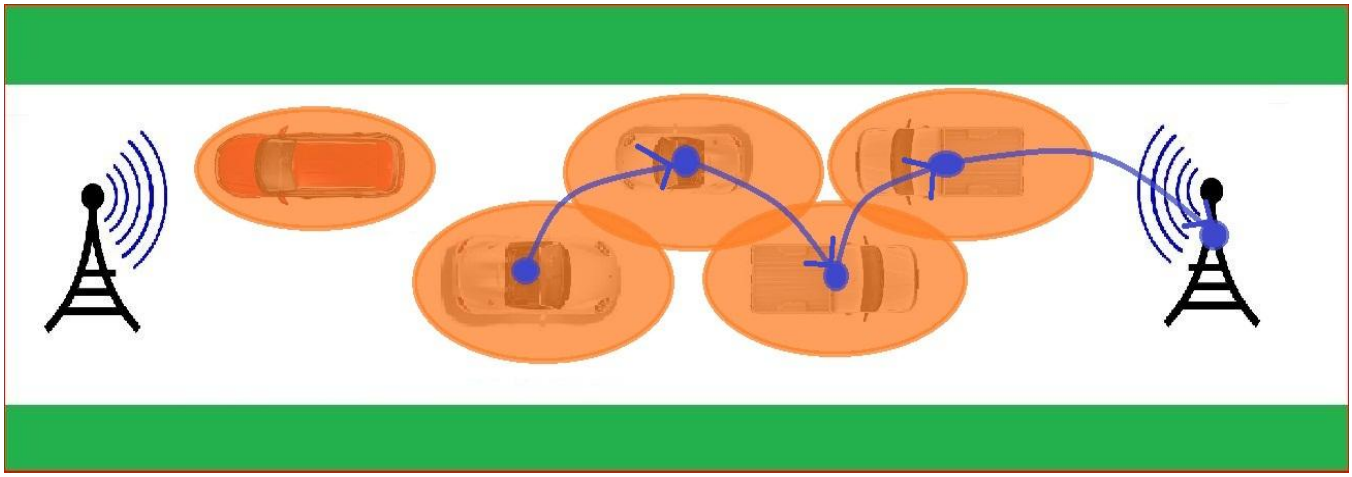


Figure 4.1: Wi-Fi ranges overlapping

In the above figure 4.1, we can see that the vehicles are overlapping their Wi-Fi ranges while moving or passing each other in highway road. Orange circles represent the Wi-Fi ranges here.



(a) Data is passing from sink to a vehicle



(b) Data is reaching its destination to other sink

Figure 4.2: Data passing

So here in above figure 4.2, we can see that data is passing from left sink and then one vehicle to another vehicle after connecting their Wi-Fi. Finally it sends data to the right sink. So by this, data can be transferred.

Speed: We ran our simulation basically for the speeds of 36 km/h. We considered the speed to be constant for the whole time.

4.2 Data Delivery Schemes:

There are 3 ways to deliver data. These are:

1. One way one direction
2. Multi-hop one direction
3. Multi-hop multi direction

4.2.1 One Way One Direction:

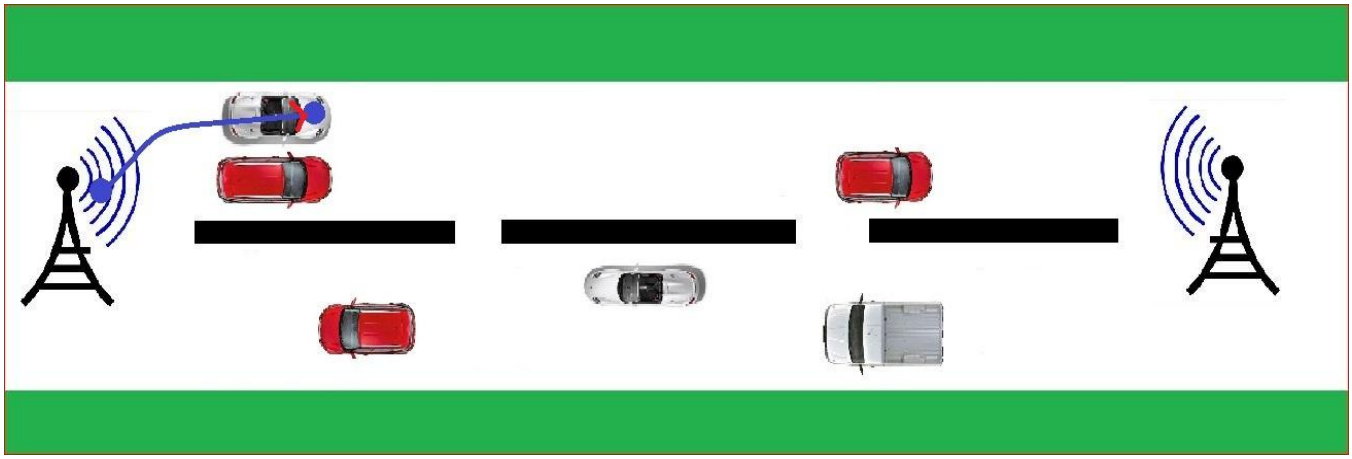
One way one direction is the first of our three schemes for delivering data from one place to another. Here direction refers to data direction not conventional direction like north, south etc. In one way one direction, the direction of data does not change. We already know the basic strategy is to 'store, carry and forward'. But in one way one direction there is no forwarding of data except for delivering it to the sink. Here there is no vehicle to vehicle data transfer.

A vehicle (car, truck, motorcycle, cycle etc.) collects data from the sink, stores the data in its storage system and moves towards its destination. On its journey it does not forward data to any other vehicle even if the other vehicle is within the Wi-Fi range. This is the basic difference between this scheme and the other two schemes. In other schemes data is forwarded from one vehicle to the other vehicle in hop by hop manner. But we are going to discuss it later elaborately.

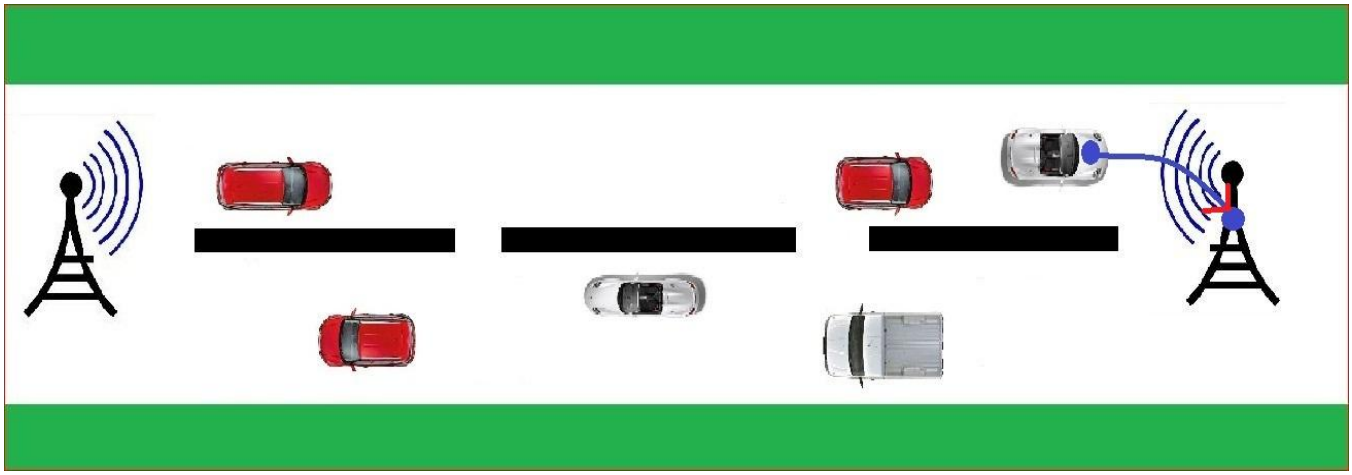
In one way one direction there is no hopping of data from one vehicle to the next vehicle. Here hopping occurs in only twice-

a) While receiving data from the sink and

b) While delivering data to the sink.



(a) Data starts to pass from sink to vehicle



(b) Data reaches its destination in only forward direction

Figure 4.3: One way one direction

In the figure 4.3, we see an example of one way one direction. Here we see that, there are two sinks A and B and they are far apart from each other. Every vehicle collects its data from the sinks and is carrying its own data and proceeding towards their respective destination.

Advantages: Less chance of data loss and data security is ensured.

Disadvantages: Data rate is slow.

4.2.2 Multi-Hop One Direction:

In multi-hop one direction a vehicle collects data from one sink and if it finds another vehicle moving in the same direction and within its Wi-Fi range then it forwards the data to the next vehicle and the data is then stored on the second vehicle. After one hopping, if there are no vehicles within the Wi-Fi range, then that vehicle stores the data until it finds another vehicle. Whenever the second vehicle is in contact with another vehicle it forwards the data to that vehicle. This hopping or forwarding continues until the data reaches the destination (the sink). In multi-hop one direction every vehicle receives data from the sink and they move forward and keep checking for a vehicle ahead of them and they measure the Wi-Fi range. If their Wi-Fi range overlaps then they connect with each other. The vehicle which is lagging behind forwards the data to the next vehicle.

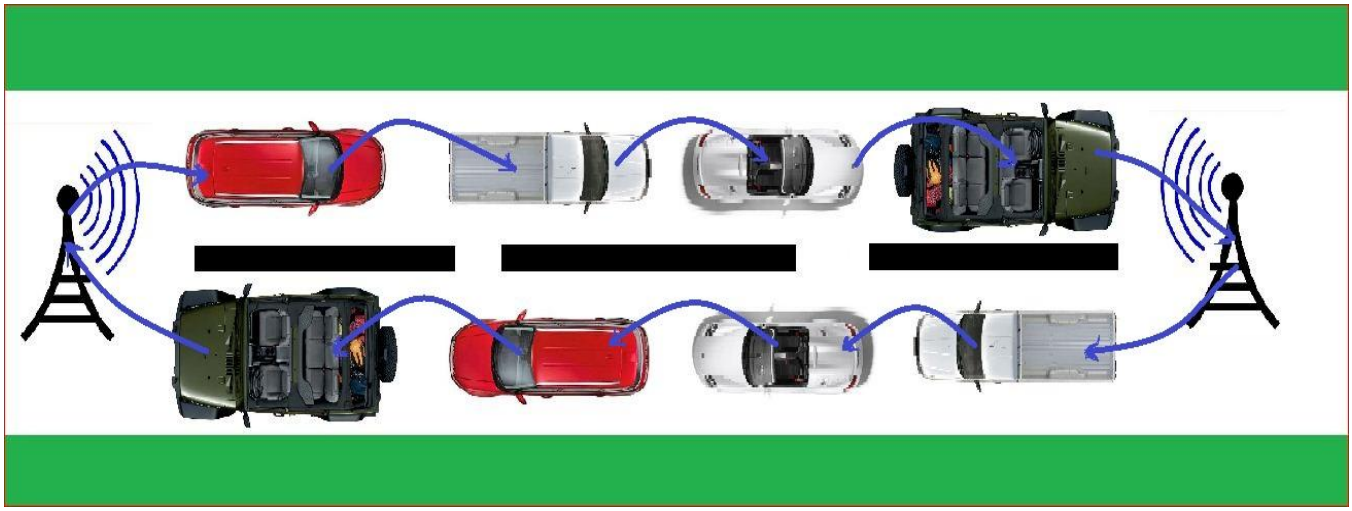


Figure 4.4: Multi-hop one direction

Here (figure 4.4) is an example of multi-hop one direction data transfer. Like in the previous case there are two sinks A and B. There are some vehicles on the road-some are moving from sink A to sink B and some are moving from sink B to sink A. every vehicle is carrying its own data as we see in the figure. Whenever two vehicles are within the Wi-Fi range of each other we see hopping of data as described earlier.

Advantage: Data delivery rate is faster.

Disadvantage: Data confidentiality can be exposed.

4.2.3 Multi-Hop Multi-Direction:

In multi-hop one direction there is no hopping of data to the vehicles of the opposite direction but in multi-hop multi-direction data hops into the vehicle of the same direction as well as vehicles of the opposite direction.

While moving towards destination, every vehicle tries to hop its data to a vehicle that is ahead it and on the same direction. If there is no vehicle on the same direction, then it tries to hop its data to a vehicle coming towards it. The vehicle from the opposite direction tries to hop the data in a vehicle of the same direction or in the opposite direction. For the case of same direction, the vehicle hops the data to a vehicle that is behind it. Because there is no point in delivering the data into a vehicle that is ahead of it. In that case the data is going to be carried into the same direction it has come from.

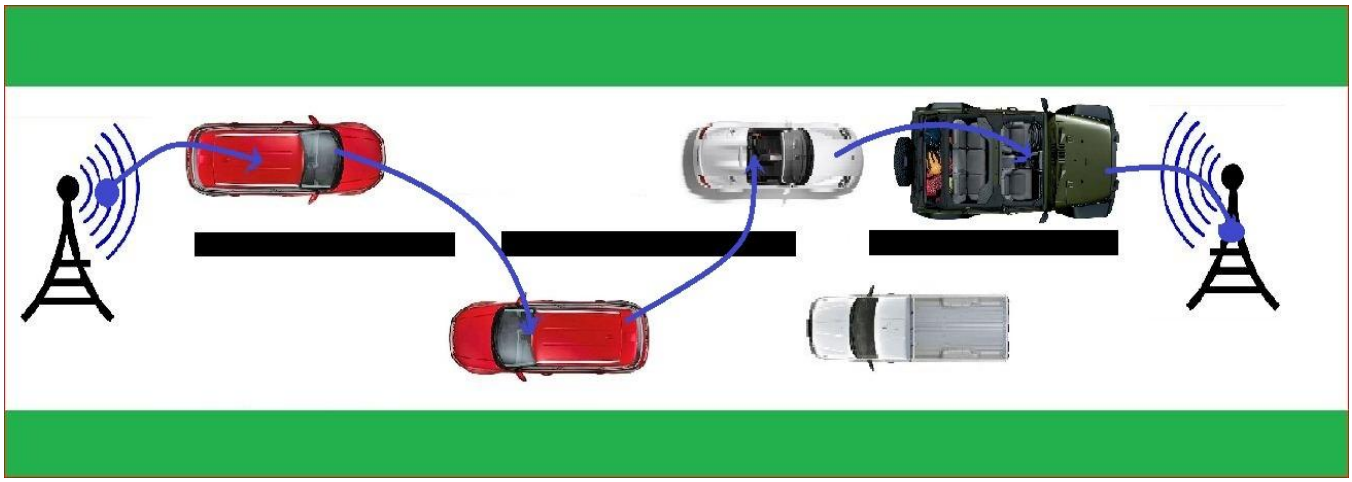


Figure 4.5: Multi-hop multi-direction

From the above figure (4.5) we see that there are four vehicles –car1, car2, car3 and car4. Car1 and car4 are moving from sink 2 to sink 1 whereas car2 and car 3 are moving from sink 1 to sink 2.

Suppose sink 2 wants to send some data to sink 1. So it passes the data to car 4. If it is one way one direction, then car 4 is going to carry the data all the way to sink A. If it is multi-hop one direction, then car 4 tries to hop the data to the next vehicle in the same direction. But

there is no vehicle available next to car 4. So it carries the data until it can pass the data to another vehicle.

Advantage: Data rate is faster than previous two delivery schemes.

Disadvantages:

• Data loss is more

• Data confidentiality is difficult to maintain.

4.3 Simulation:

For simulation we used "**NetLogo 5.0.3**" software. It is an open source and user friendly software.

4.3.1 Simulation Setup:

We built our simulator according to our model scenario. We selected the road length to be 5 kilometers. The road is a two lane road. We chose car and truck as our default vehicles. The Wi-Fi devices have Wi-Fi range of 250 meters. Every sink generates data and delivers it to the other sink. That means one sink generates data which is delivered to the other sink via all the three schemes one way one direction, multi-hop one direction and multi-hop multi-direction separately. We fixed our model setup that means for all three schemes the position of all vehicles were fixed in order to maintain similarity. The speed of all the vehicles was constant during the whole simulation.

No	Parameters	Value
01.	Length of the road	5 kilometers
02.	Number of data (for a single sink)	20 and 30
03.	Speed of the vehicle (km per hour)	7,15,30,36
04.	Wi-Fi range	250 meter

Table 4.1: Simulation Setup

We ran our simulation on a platform (Personal Computer) with the following configuration:

1.	Machine name	EXTREME
2.	Operating System	Windows 7 Professional 64-bit (6.1, Build 7600)
3.	Language	English (Regional Setting: English)
4.	System Manufacturer	BIOSTAR Group
5.	System Model	G41-M7
6.	BIOS & DirectX Version	Default System BIOS & DX 11
7.	Processor	Intel(R) Core(TM)2 Quad CPUQ8400 @ 2.66GHz (4 CPUs), ~2.7GHz
8.	Memory	4096MB RAM (OS-4062 MB RAM)
10.	Page File	1159MB used, 6961MB available
11.	Windows Dir	C:\Windows
12.	System DPI Setting	96 DPI (100 percent)
13.	DxDiag Version	6.01.7600.16385 32bit Unicode

Table 4.2: system Configuration

Chapter 5

Results and Discussions

We ran our simulation for road length of 5 km and vehicle speed was chosen to be 7 km/h, 15 km/h, 30 km/h and 36 km/h.

For 7 km per hour we have got this data:

First, 20 data which was sent by sink 1 and received by sink 2.

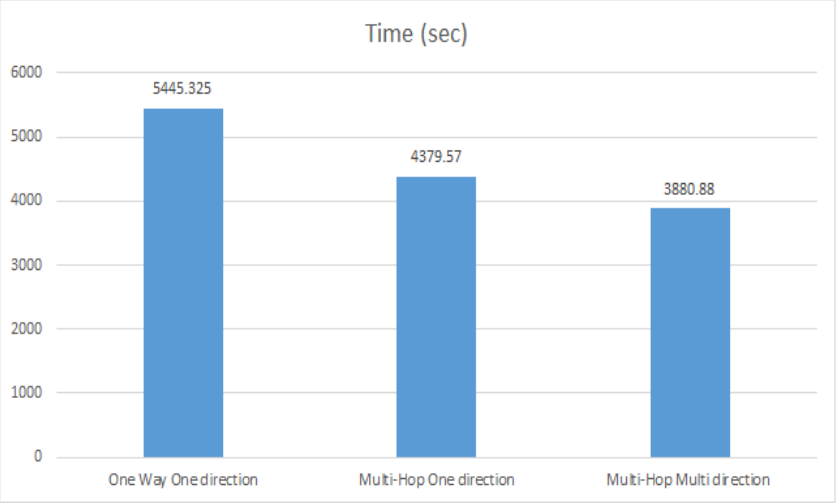
Name of the scheme	Number of sent data by Sink1	Number of received data by Sink2	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	20	20	5445.325	**0.0037**
Multi-hop one direction	20	20	4379.57	**0.0042**
Multi-hop multi-direction	20	20	3880.88	**0.005**

Table 5.1: Data collection for speed 7 km/h and road length of 5 km

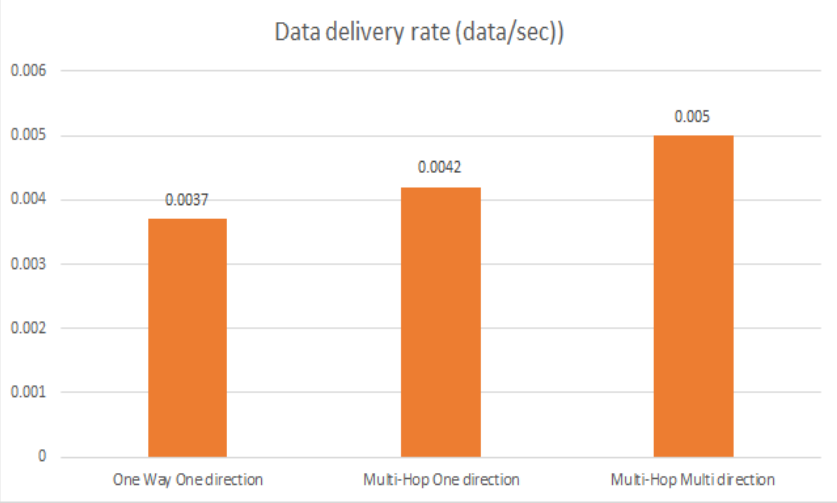
From table 5.1, we found that data delivery rate was highest for multi-hop multi direction and lowest for one way one direction. Normally for 7 km per hour, time should be less in real life calculation. But for the simulation, we got these results. In the table, we saw that taken time was higher for one way one direction and lower for multi-hop multi direction. Data delivery rate was decreasing as the time increased for certain amount of data.

We took 20 data which was sent by sink 1 and received by sink 2. As this, 30 data which was sent by sink 2 and received by sink 1. How much data we took was random selection. We could do that for 100 or 1000 data. So there would be change in taken time and data delivery rate.

Graphs (From Table 5.1):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

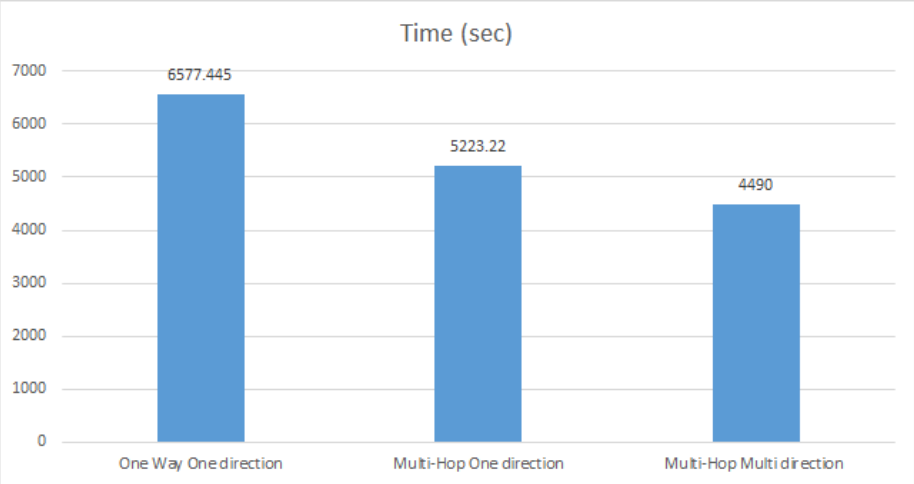
Second, 30 data which was sent by sink 2 and received by sink 1.

Name of the scheme	Number of sent data by Sink2	Number of received data by Sink1	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	30	30	6577.445	**0.0046**
Multi-hop one direction	30	30	5223.22	**0.0053**
Multi-hop multi-direction	30	30	4490	**0.0065**

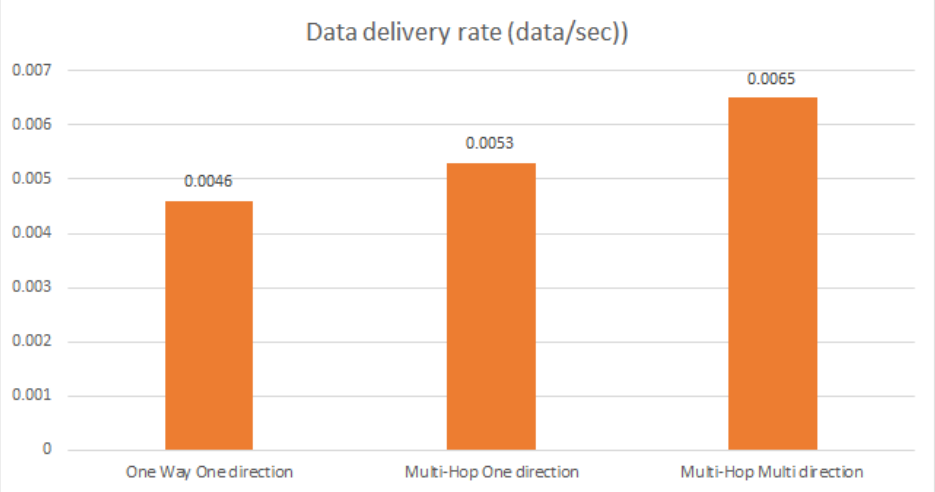
Table 5.2: Data collection for speed 7 km/h and road length of 5 km

From table 5.2, we found that data delivery rate was highest for multi-hop multi direction and lowest for one way one direction. But as we took 30 data there, time as well as data delivery rate changed. Data we got for 20 data was lower than we got for 30 data. So here we saw that as data increased, data delivery rate also increased for each delivery schemes. So we found that, data delivery rate and taken time was dependent on amount of data.

Graphs (Table 5.2):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

From the table 5.1, 5.2 and their graphs, we found that data delivery rate was highest for multi-hop multi-direction and lowest for one way one direction.

For 15 km per hour we have got this data:

First, 20 data which was sent by sink 1 and received by sink 2.

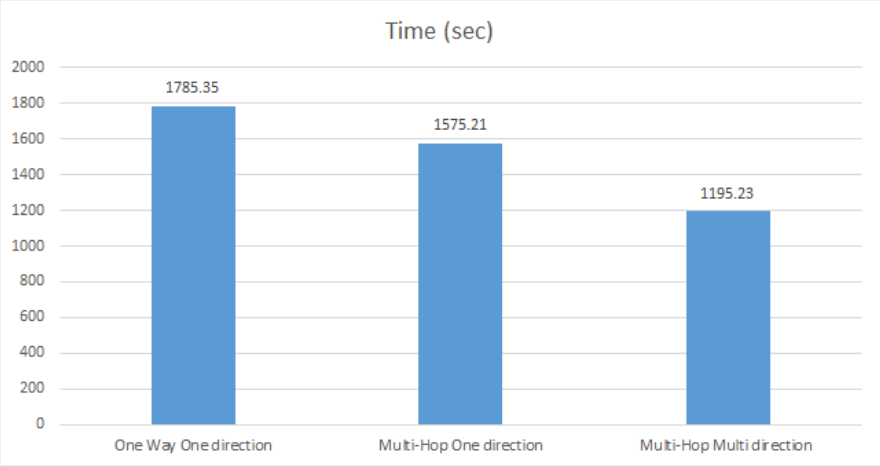
Name of the scheme	Number of sent data by Sink1	Number of received data by Sink2	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	20	20	1785.35	**0.011**
Multi-hop one direction	20	20	1575.21	**0.04**
Multi-hop multi-direction	20	20	1195.23	**0.07**

Table 5.3: Data collection for speed 15 km/h and road length of 5 km

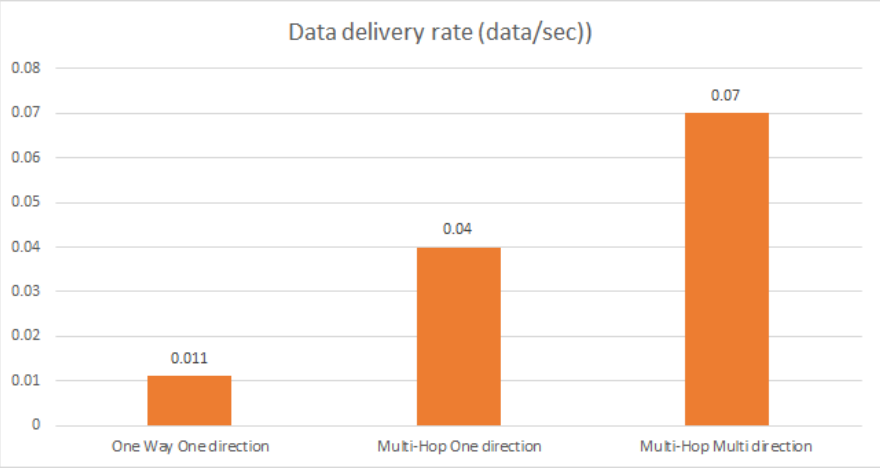
From table 5.3, we found that for 15 km per hour, data delivery rate was highest for multi-hop multi direction and lowest for one way one direction. Practically or in reality, more or less time was same. But for the simulation, we got these results.

In the table, we saw that taken time was higher for one way one direction (**1785.35 sec**) and lower for multi-hop multi direction (**1195.23 sec**). Data delivery rate was decreasing as the time increased for 20 data sent by sink 1 and received by sink 2. In multi-hop multi direction scheme, data delivery rate was higher (**0.07 data/sec**).

Graphs (Table 5.3):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

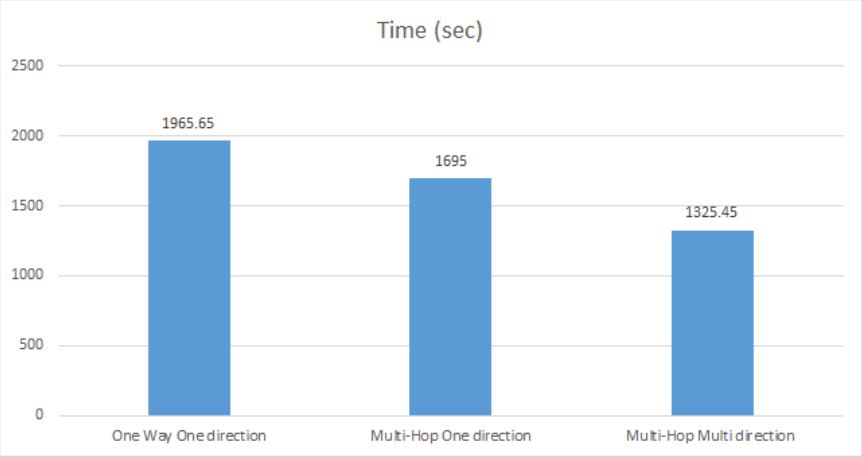
Second, 30 data which was sent by sink 2 and received by sink 1.

Name of the scheme	Number of sent data by Sink2	Number of received data by Sink1	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	30	30	1965.65	**0.03**
Multi-hop one direction	30	30	1695	**0.06**
Multi-hop multi-direction	30	30	1325.45	**0.13**

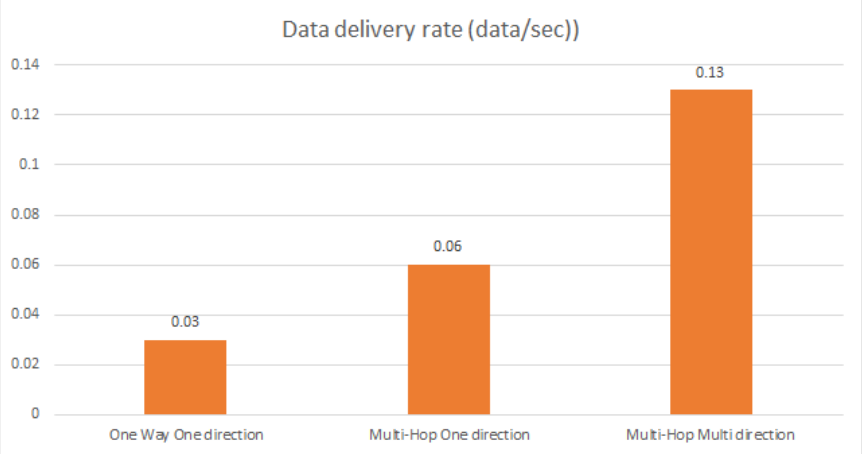
Table 5.4: Data collection for speed 15 km/h and road length of 5 km

For the above table 5.4, we found that for 30 data, taken time changed a bit and as well as data delivery rate. There data delivery rate for multi-hop multi direction scheme was higher (**0.13 data/sec**) than other two schemes but a little bit larger than value of previous taken delivery rate for 20 data. So we saw that as data increased from 20 to 30, data delivery rate was increased.

Graphs (Table 5.4):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

From the table 5.3, 5.4 and their graphs, we found that data delivery rate was highest for multi-hop multi-direction and lowest for one way one direction.

For 30 km per hour we have got this data:

First, 20 data which was sent by sink 1 and received by sink 2.

Name of the scheme	Number of sent data by Sink1	Number of received data by Sink2	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	20	20	1470	**0.013**
Multi-hop one direction	20	20	726	**0.03**
Multi-hop multi-direction	20	20	348	**0.06**

Table 5.5: Data collection for speed 30 km/h and road length of 5 km

From table 5.5, we found that for 30 km per hour, data delivery rate was highest for multi-hop multi direction and lowest for one way one direction. In the table, we saw that taken time was higher for one way one direction (**1470 sec**) and lower for multi-hop multi direction (**348 sec**). Data delivery rate was decreasing as the time increased for 20 data sent by sink 1 and received by sink 2. In multi-hop multi direction scheme, data delivery rate was higher (**0.06 data/sec**).

Secondly, 30 data which was sent by sink 2 and received by sink 1.

Name of the scheme	Number of sent data by Sink2	Number of received data by Sink1	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	30	30	1875	**0.016**
Multi-hop one direction	30	30	798	**0.04**
Multi-hop multi-direction	30	30	411	**0.08**

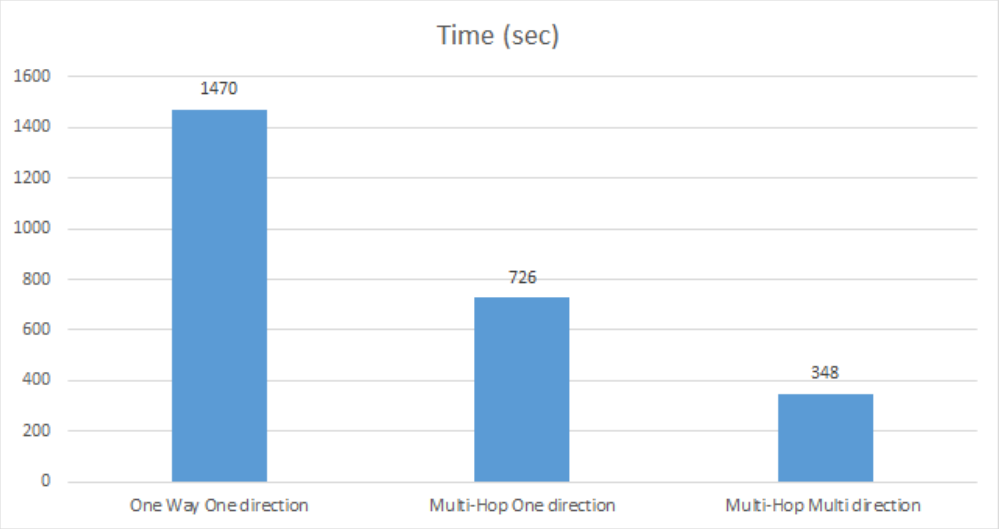
Table 5.6: Data collection for speed 30 km/h and road length of 5 km

From table 5.6 and their graphs, we found that the data delivery rate was highest in multi-hop multi-direction and lowest in one way one direction. We also saw that data delivery rate increased as speed of vehicles increased.

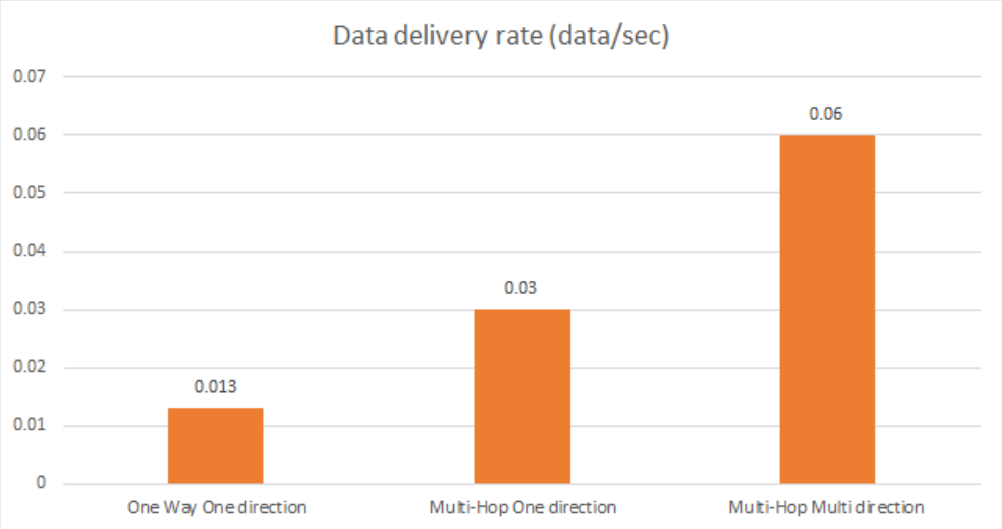
We plotted the relevant graphs as well. All the graphs are added below for better understanding of the topic.

Here are the two graphs (30 km per hour)-

(i). Sent by sink 1 and received by sink 2

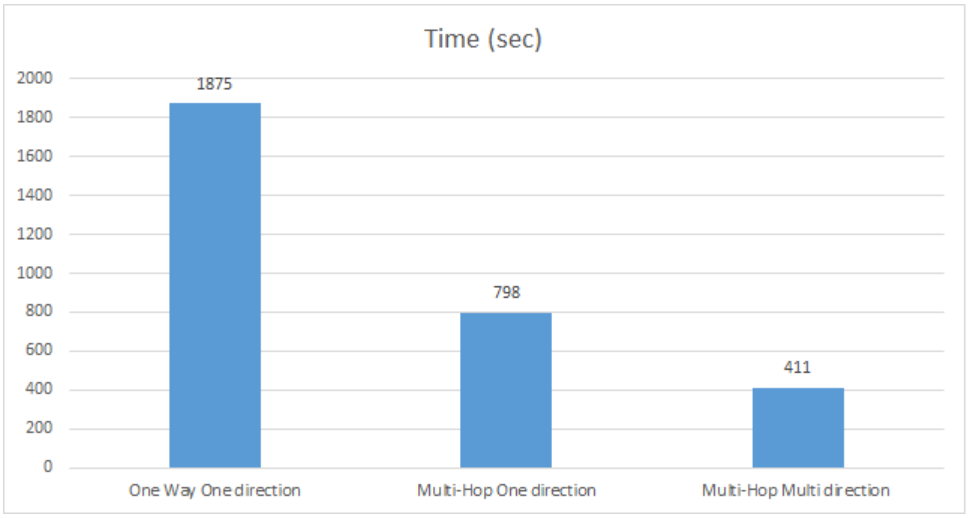


(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)

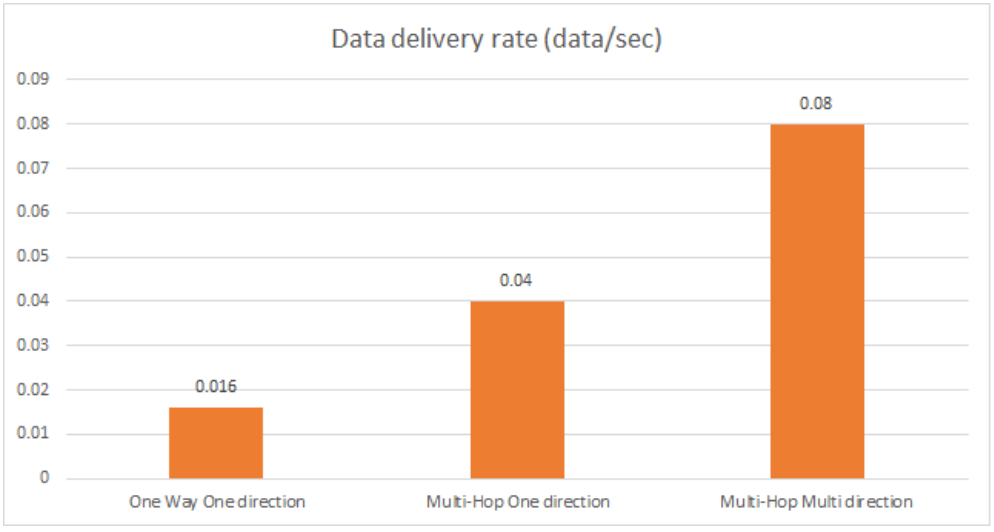


(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

(ii). Sent by sink 2 and received by sink 1



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

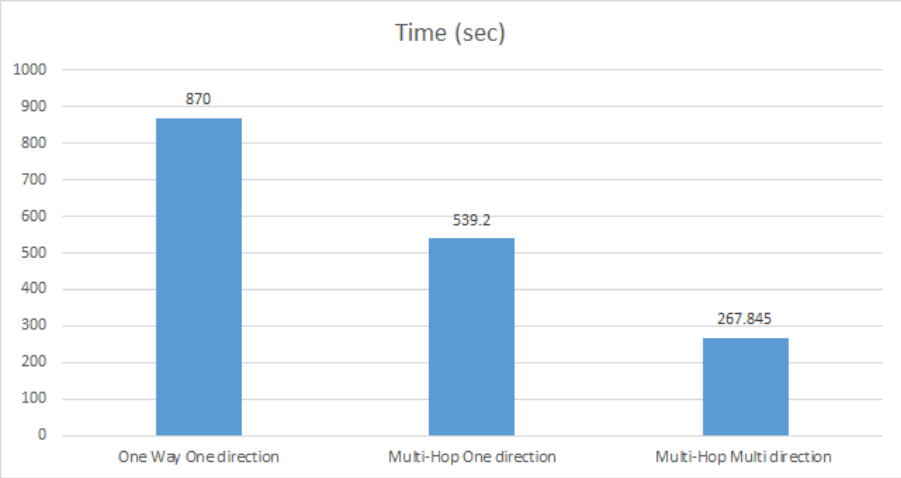
For 36 km per hour we have got this data:

Name of the scheme	Number of sent data by Sink1	Number of received data by Sink2	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	20	20	870	**0.02**
Multi-hop one direction	20	20	539.2	**0.037**
Multi-hop multi-direction	20	20	267.845	**0.07**

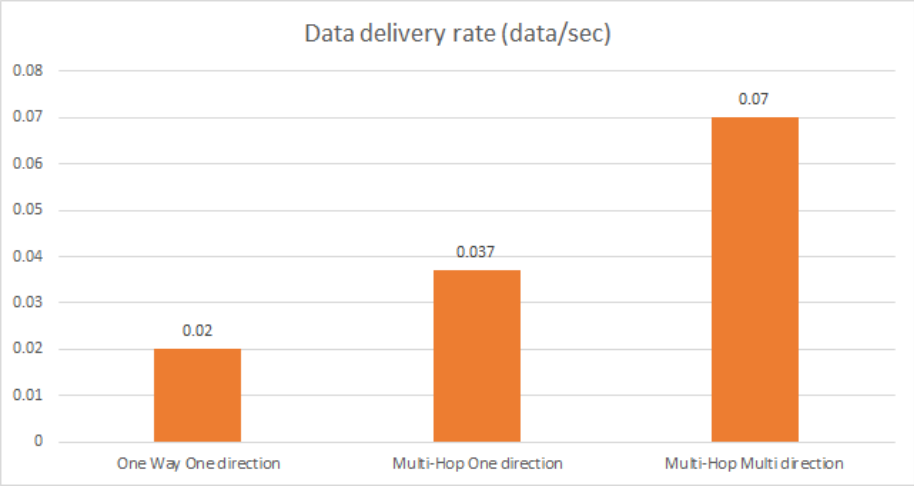
Table 5.7: Data collection for speed 36 km/h and road length of 5 km

From table 5.7, we found that for 36 km per hour, data delivery rate was highest for multi-hop multi direction and lowest for one way one direction. But here we some differences from other speeds. We saw that as we increased the speed, the taken time decreased. In the table, we saw that taken time was higher for one way one direction (**870 sec**) and lower for multi-hop multi direction (**267.845 sec**). These data was higher for previous cases. Data delivery rate was decreasing as the time increased for 20 data sent by sink 1 and received by sink 2. In multi-hop multi direction scheme, data delivery rate was higher (**0.07 data/sec**).

Graphical representation (from table 5.7):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

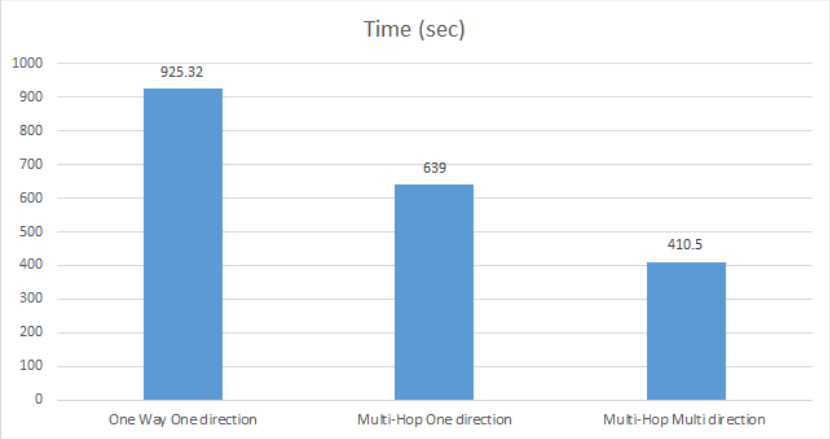
Second, 30 data sent by sink 2 and received by sink 1:

Name of the scheme	Number of sent data by Sink2	Number of received data by Sink1	Total time (sec)	Average data delivery rate (data/sec)
One way one direction	30	30	925.32	**0.032**
Multi-hop one direction	30	30	639	**0.047**
Multi-hop multi-direction	30	30	410.5	**0.073**

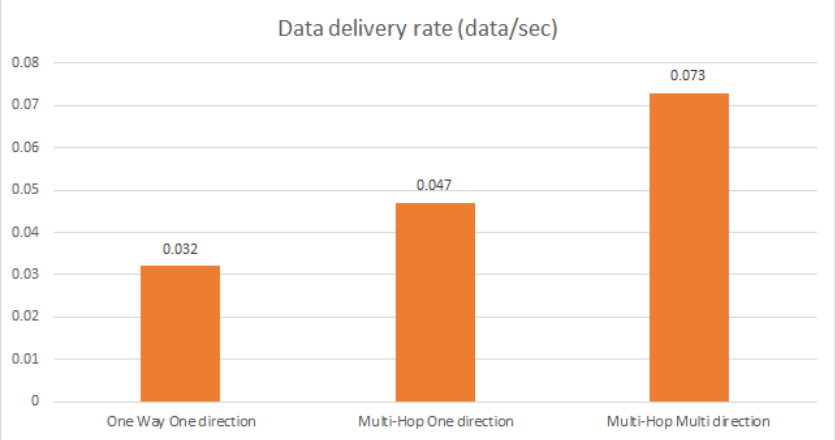
Table 5.8: Data collection for speed 36 km/h and road length of 5 km

From table 5.8, we used 30 data which was sent by sink 2 and received by sink 1. What we found was the data delivery rate was highest in multi-hop multi-direction and lowest in one way one direction, but had lower value than the previous data from table 5.7 for 20 data.

Graphical representation (from table 5.8):



(a) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents time (sec)



(b) In above graph, 'x-axis' represents data delivery schemes and 'y-axis' represents data delivery rate (data/sec)

Comparison:

Above these tables and graphical representations for 7 km/h, 15 km/h, 30 km/h and 36 km/h, we visualized that for multi-hop multi direction scheme, data delivery rate was the highest and taken time was lowest. It matched with the theory. We simulated 10 times for every speeds. So far we had understood that multi-hop multi direction scheme was the best option to transfer data. But this scheme has many problems. Though data rate is faster for multi-hop multi direction scheme but data loss is more here than other two schemes. Maintaining security i.e. data confidentiality is more complex here. So we are trying to solve this.

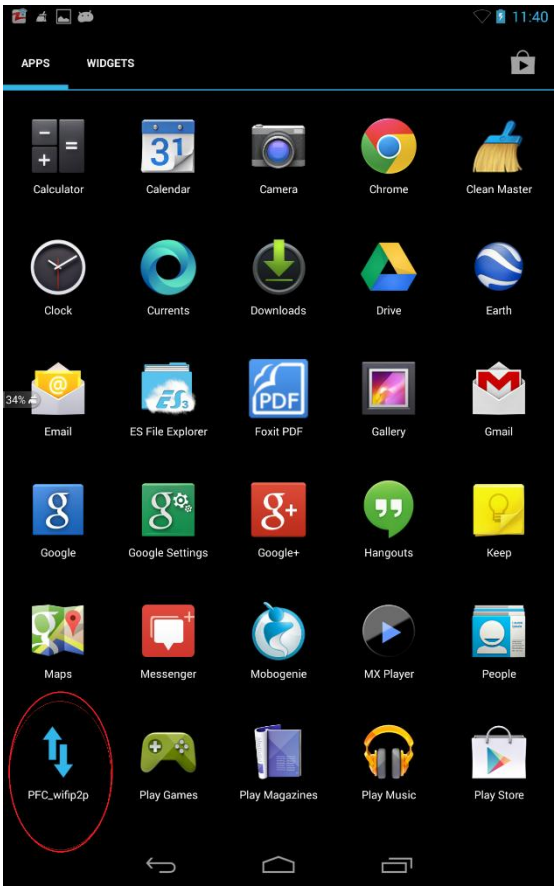
Practical implementation:

For practical implementation we took two Android devices. Then we developed an application suitable for Android 4.1 or 4.1+ versions. By this we did connect those devices by their Wi-Fi and they passed their data from one to another.

For example, we named the application as **IUTdtn_wifip2p.apk**

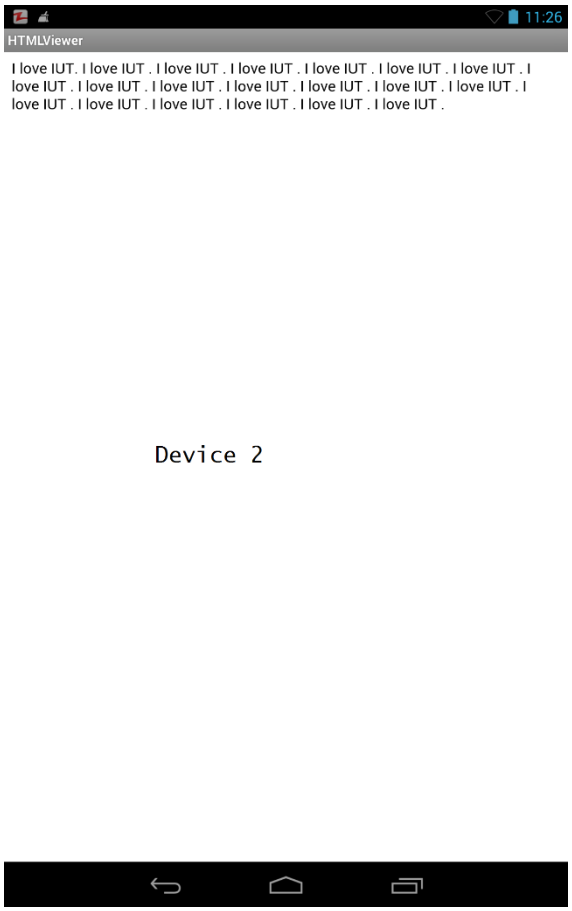
These are some screenshots which we have taken through the processes.

In below picture, we can see the installed application (in red circle).



We considered that both devices were already connected. So just had to send data file. But first we have to search for the devices. Though our motivation doesn't fulfil this, we are trying to peer the devices automatically. It is a very big challenge for us to do it. So we will take it as our future work.

After that when we selected "**Send data**" option, data started to deliver to device 2 (below image):



So far we did this. But our motivation was not it. We want to transfer data between two devices when they are moving (like vehicles move in highway road). To achieve our goal, this application will not help. So to achieve our motivation of the thesis, we need to develop our application. For now, we have to search for the devices and connect with them manually. But we wanted to send data between two devices automatically. It means that when two devices will come closer or come in their Wi-Fi ranges, they will transfer their data within that time. So time and speed is a very important issue to be considered here. We are trying to develop the application.

Chapter 6

Conclusion and Future Plan

Though our research work has showed some performances but not good, there can be done a lot of improvements. There are some complexities that can be handled for future research on this topic. We are trying to develop the application and make it more suitable for practical implementation. But to do this perfectly, we have to face some challenges. We tried to give some extensions. Those are-

Wi-Fi connections and its ranges. Without good Wi-Fi coverage, we can't implement our research. Speed of the vehicles is a very big issue for this. Because speed varies time to time. So without perfect match, we can't transfer our data. In above work, we are only able to transfer data file. So transferring different types of data can be a complex work to do. Security assurance is a very big challenge for this and it must be maintained. For such limitations we don't expect perfect accuracy for our thesis.

Now we can send data between two devices when they overlaps their Wi-Fi ranges. But we are working on peering issues. It's our first priority to establish connection devices without any permission, like they don't have to connect manually. So it can be a great challenge to pass the data in high speed and in extreme condition i.e. natural calamities. Ad-hoc DTNs is a technology that is very new to the developing countries i.e. Bangladesh. If we can overcome these problems completely, there can be many extensions for our topic in future research and we can implement something bigger for our country. So we are trying to get better results.

References:

[1] Perkins, Charles E, "Ad hoc networking", Addison-Wesley Professional, perkins2008ad, 2008.

[2] Kopp, Carlo, "Ad Hoc Networking", Systems Journal, kopp1999ad, pp: 33—40, 1999.

[3] RFC 4838, V. Cerf, S. Burleigh, A.Hooke, L.Torgerson, NASA Jet Propulsion Laboratory (NASA/JPL), R. Durst, K. Scott, The MITRE Corporation, K. Fall, Intel Corporation. , H. Weiss, SPARTA, Inc. "Delay – Tolerant Networking Architecture", April 2007.

[4] Lloyd Wood, et.al, "Use of Delay Tolerant Networking Bundle Protocol from Space", IAC – 08 – B2.3.10, Global Government Solutions Group, Cisco Systems, UK.

[5] Hervé Ntareme, Marco Zennaro, Björn Pehrson, "Delay Tolerant Network on smartphones: Applications for Communication challenged areas", published in Extremecom 2011, Brazil, September 2011.

[6] Joshua B. Schoolcraft, Scott C. Burleigh, Ross M. Jones, E. Jay Wyatt, J. Leigh Torgerson, "The Deep Impact Network Experiments – Concept, Motivation and Results", Jet Propulsion Laboratory, California Institute of Technology, 2010.

[7] http://www.nasa.gov/mission_pages/station/research/experiments/1002.html, this content was provided by Kim Nergaard, and is maintained in a database by the ISS Program Science Office, 05.23.13.

[8] John Heidemann, Milica Stojanovic and Michele Zorzi, "Underwater sensor networks: applications, advances and challenges", Phil. Trans. R. Soc. A (2012) 370, pp: 158–175, 2012.

[9] A. MacMahon, S. Farrell. "Delay-And Disruption-Tolerant Networking," IEEE Internet Computing, vol. 13, no. 6, pp. 82-87, Nov/Dec. 2009.

[10] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", Intel Research Technical. Report IRB-TR-03-003, Feb 2003.

[11] K. Fall, S. Farrell, "DTN: An architectural retrospective", IEEE Journal on selected Areas in Common, Vol.26, no.5. pp. 828-826, June 2008.

[12] Z. J. Haas et al., Guest Editorial, IEEE JSAC. "Special Issue on Wireless Networks". Vol. 17, No. 8, Aug. 1999, pp. 1329 – 32.

[13] R. Handorean et al., "Accommodating Transient Connectivity in Ad Hoc and Mobile Settings," Pervasive 2004, Apr. 21–23, 2004, Vienna, Austria, pp. 305–22.

[14] W. Zhao et al., "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks," Proc. 5th ACM Int'l. Symp. Mobile Ad Hoc Net. And Comp., ACM Press, 2004, pp. 187–98.

[15] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges," IEEE Communications Surveys and Tutorials, vol. 8(1), pp. 24-37, 2006.

[16] Cerf, Vinton and Burleigh, Scott and Hooke, Adrian and Torgerson, Leigh and Durst, Robert and Scott, Keith and Fall, Kevin and Weiss, Howard, "Delay-tolerant networking architecture", cerf2007delay, RFC4838, April, 2007.

[17] Y. Matsushita, M. Sakuma, H. Nishigaki, N. Miyazaki, and I. Yoshida, "An Overall Network Architecture Suitable for Implementation with either Datagram or Virtual Circuits Facilities," SIGCOMM Comput. Commun. Rev., vol. 8, no. 3, pp. 5–24, 1978.

[18] M. Seligman, K. Fall, and P. Mundur, "Alternative custodians for congestion control in delay tolerant networks," inProc. ACM SIGCOMM Workshop on Challenged Networks. New York, NY, USA: ACM Press, 2006, pp. 229–236.

[19] Campos, C.A.V., Otero, D.C. & de Moraes (2004, March), Realistic individual mobility Markovian models for mobile ad hoc networks," Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, vol.4, no., pp.1980-1985 Vol.4, 21-25.