ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

STUDY ON VEHICULAR AD-HOC DELAY TOLERANT NETWORK

By

A.S.M. Saifuddin (092419)

M. Al Mamun (092439)

Md.Omar Faruk Chowdhury (092440)

A Dissertation

Submitted in Partial Fulfillment of the Requirement for the

Bachelor of Science in Electrical and Electronic Engineering

Academic Year: 2012-2013

Department of Electrical and Electronic Engineering

Islamic University of Technology (IUT)

A Subsidiary Organ of OIC

Dhaka, Bangladesh

A Dissertation on,

STUDY ON VEHICULAR AD-HOC DELAY TOLERANT NETWORK

Submitted by

A.S.M. Saifuddin	M. Al Mamun	Md. Omar Faruk Chowdhury

Approved by

Dr. Md. Shahid Ullah

Professor & Head of the

Department of EEE, IUT.

Dr. Khondokar Habibul Kabir

Thesis Supervisor

Assistant Professor

Department of EEE, IUT.

To our family

Acknowledgment

At first we would like to express our sincere gratitude to Almighty Allah, the most merciful and beneficent. Without Allah's mercy we would not be able to finish our work.

Then we want to thank our supervisor Dr. Khondokar Habibul Kabir for his guidance, patience and support during our thesis.

Next we want to thank our family members for their love and inspiration without which we would have never been at the point where we stand now.

Abstract

STUDY ON VEHICULAR AD-HOC DELAY TOLERANT NETWORK

Data networks allow data transfer between network nodes which is essential for modern communication. Such data networks require fixed infrastructure. To establish such infrastructure a lot of financial resources are required. The mission of this dissertation is to uniquely identify that data network can also be established in infrastructure-less scenario such as highways.

We declare three schemes for data delivery via moving vehicles in highway data network. One way one direction, multi-hop one direction and multi-hop multi-direction are the three schemes proposed by us. We effectively transferred data using these schemes by software simulation. Among these three schemes, multi-hop multi-direction has the highest data delivery rate. Our ultimate target is to practically implement our work where simulation results are going to help us to a great extent.

CONTENTS

List of Tables

List of Figures

Chapter 1

Introduction

Networking is essential for communication. Networking allows network nodes to exchange data. Absence of network or data network means no communication whatsoever. For creating any network, infrastructure is essential. Creating a network in an area without any fixed infrastructure is a challenge.

We want to create networks to transfer data in infrastructure-less area. Such scenario can be in highways where there is no fixed structure or tower to transfer data, and hence, no data networks.

In highways there are moving vehicles. Vehicles are moving from one place to another continuously. If we can use these vehicles to create a network, then we can easily transfer data between two distant places without any fixed infrastructure. Fixed infrastructure like towers, antenna etc costs a lot of money. So a vehicular network can save a lot of money apparently.

The main challenge in creating such a network is the intermittent connections between the high speed vehicles. Other challenges may include sparsity of vehicles, storage system, power supply etc. To create network in such scenario, we can use Ad hoc Delay Tolerant Network. 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 want to establish effective data delivery between two distant places using three different schemes- one way one direction, multi-hop one direction and multi-hop multi-direction.

In chapter 2 and chapter 3 we discuss the background of our thesis work. In chapter 2 we study about delay tolerant net work and in chapter 3 we study about ad-hoc networking. Chapter 4 is about our proposed model and methodology of our work and finally we validate our analytic approach via "NetLogo" simulation. In chapter 5 we study the results obtained from our simulation. In chapter 6 we summarize and conclude our dissertation.

Chapter 2

Delay Tolerant Network

Delay tolerant network is a networking architecture that is useful when there is lack of continuous connectivity between the networking nodes. It is also known as disruption tolerant network.

2.1 History of delay-tolerant networking:

In the 1970s, spurred by the decreasing size of computers, researchers began developing technology for routing between non-fixed locations of computers. 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.

Concurrently with (but separate from) the MANET activities, DARPA had funded NASA, MITRE and others to develop a proposal for the Interplanetary Internet (IPN). Internet pioneer Vint Cerf and others developed the initial IPN architecture, relating to the necessity of networking technologies that can cope with the significant delays and packet corruption of deep-space communications. 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 [1]. 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. This field saw many optimizations on classic ad hoc and delay-tolerant networking algorithms and began to examine factors such as security, reliability, verifiability, and other areas of research that are well understood in traditional computer networking.

2.2 Reason behind approaching for DTN:

The existing TCP/IP based Internet service model provides end-to-end inter-process communication using a concatenation of potentially dissimilar link-layer technologies. The standardization of the IP protocol and its mapping into network-specific link-layer data frames at each router supports interoperability using a packet-switched model of service. Although often not explicitly stated, a number of key assumptions are made regarding the overall performance characteristics of the underlying links in

order to achieve this service: an end-to end path exists between a data source and its peer(s), the maximum round-trip time between any node pairs in the network is not excessive, and the end-to-end packet drop probability is small. Unfortunately, a class of challenged networks, which may violate one or more of the assumptions, are becoming important and may not be well served by the current end-to-end TCP/IP model. In this case we go for Delay Tolerant Networks.

2.3 Basic Concept of DTN:

Initially developed for Deep Space Communication (Inter Planetary Internet), the Delay-Disruption Tolerant Network communication model can also be used in Wireless (Terrestrial) environments, both in Military and Civilian Applications. The main difference between the Space & Terrestrial environments can be accredited to the fact that the space contacts communications are scheduled and predictable while the terrestrial one's are more opportunistic in nature [2] and the networking model like Delay-tolerant networks can provide efficient communication in spite of challenging environments. The Traditional TCP/IP Protocol suite has served well the Internet & Networking communications till today, however there are new and challenging environments and applications where the internet protocols perform poorly (or) cannot be used at all. In such crucial environments, the DTN approach can offer a viable alternative for realizing communication. Notable feature of wireless DTN feature is that, the architecture not only includes Radio Frequency (RF), but also ranges like Ultra Wide Band (UWB), Free Space Optical and Acoustic (SONAR or Ultra Sonic) technologies. Utilizing the DTN approach requires significant effort developing additional functionality and integrating them. Delay-Disruption Tolerant networks make use of "Store – and – Forward" technique within the network in order to compensate Intermittent Link Connectivity. 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. Recent active research area, DTN seeks to address technical issues in the network that lack continuous network connectivity. Ex: remote areas with no proper infrastructure. With tremendous increase in usage; the wireless networks are witnessing several deployment issues across various extreme environments where they suffer from different level of link disruption depending upon the severity of operating conditions. In all the cases, the operation requirements are differently altered and their performance is negatively altered rendering them Heterogeneous nature.

The DTN networks reliably advances wireless traffic despite hostile conditions, jamming activity or moved or damaged nodes. While traditional IP networks relay on end-to-end connectivity, which means that data can be sent only when there is an identifiable path all the way to the destination, DTN continues to advance data even when there's no complete, identifiable path to the destination. DTN uses intermittently available links to communicate opportunistically. The information are organized into bundles rather than packets and routed through intelligent "custodians" that augment traditional routers. These custodians advance the bundles to the next node on the way to their destination. 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.

2.4 Characteristics of DTN:

DTN network architecture is composed of computing systems participating in the network called "Nodes". One-way Links connects some nodes together. These links may go Up & Down over time, due to mobility, failures (or) other events.

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 [3].

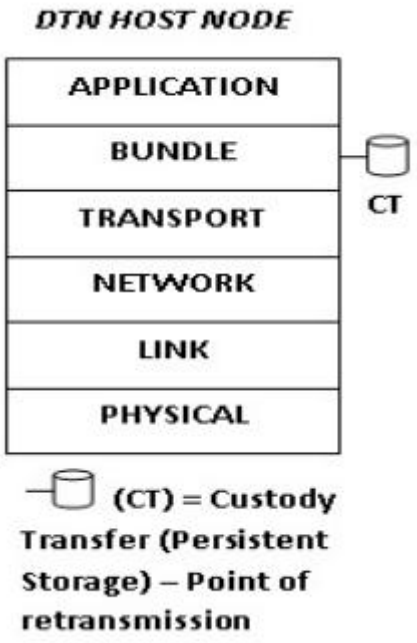


Fig 2.1: A DTN node

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. 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.

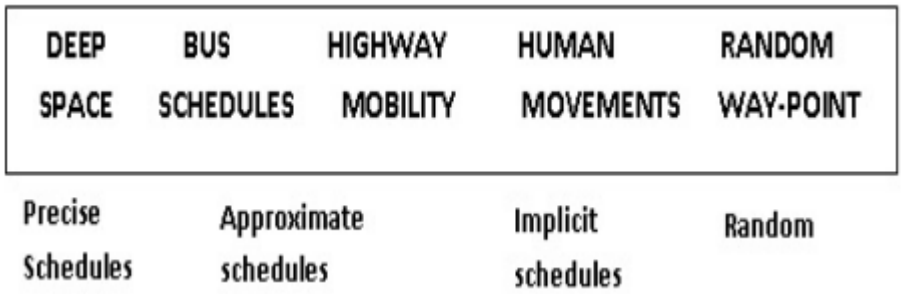


Fig 2.2: Contact Schedule Predictability

The DTN network overcomes the above hindrances structured around optionally- reliable asynchronous message forwarding of end-to-end connectivity & node resources.

2.5 Types of Contacts:

The Delay – Disruption Tolerant networks depends upon 'Contacts', which can be defined as the period of time or interval during which the Network & Communication capacity is highly positive, and the capacity can be considered as a constant. If the 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:

2.5.1 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.

2.5.2 On Demand Contact:

On – Demand Contact requires some action in order to instantiate, but then function as persistent Contact until it's terminated. A dial – up connection is an example of an On – Demand Contact.

2.5.3 Intermittent-Scheduled Contact:

A Scheduled Contact is an agreement to establish a Contact at a particular time, for particular duration ex: A Link with low – earth orbiting satellite. For the networks with substantial delays, the notion of the 'Particular time' is delay – dependent ex: a single scheduled contact between Earth and Mars would not be at the same instant in each location, but would instead be offset by the (non – negligible) propagation delay.

2.5.4 Intermittent – Opportunistic Contacts

The Opportunistic Contacts are not scheduled, but rather present themselves unexpectedly ex: an unscheduled aircraft flying overhead and beaconing, advertising its availability for communication, would present an opportunistic contact.

2.5.5 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].

2.6 Applications of DTN:

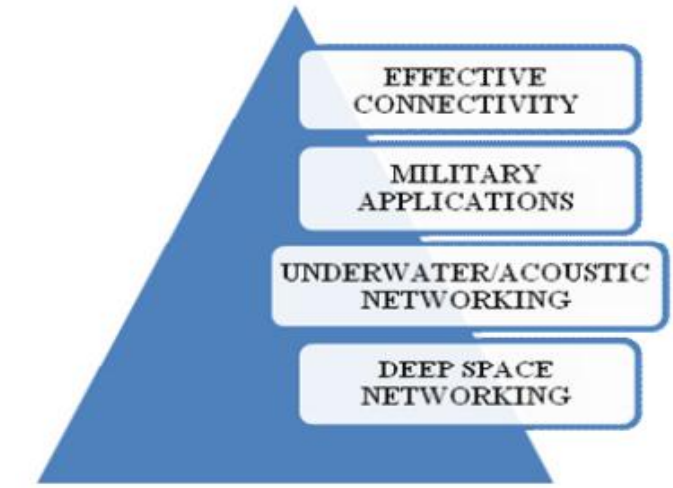


Fig 2.3: DTN Core Application

2.6.1 Deep Space Networking:

The DINET I, known as Deep Impact Network is an experimental validation of Inter – Planetary Networks, which is the NASA's implementation of Delay – Tolerant Networks. NASA (National Aeronautics & Space Administration) has successfully tested the first deep space communication network model using the DTN by transmitting around 200 space images (approx 14 MB) to and from a space craft known as EPOXI – uploaded with DTN software (functioned as a DTN router,) located more than 32 million kilometers from earth. The DTN prioritization has ensured that all high priority images were successfully delivered and no data loss or corruption found anywhere in the network. DINET II is designed to develop and validate additional DTN functionality like extended priority system, contact graph routing management and so on [5]. Along with the European Space Agency, NASA has successfully used DTN protocols to control and drive a small LEGO robot (car) at European Space Operation Centre located at Darmstadt, Germany from the International Space Station (ISS). The Multi – Purpose End – to – End Robotic Operation Network (METERON) is an application of DTN which aims at simulating selected future human

exploration scenarios including immersive remote control of a robot by an astronaut in orbit around a target object (such as Mars or Moon) [6].

2.6.2 Tactical Military Applications:

With gradual deepening and development of modern military warfare towards Network Centric Warfare (NCW), the performance of Networks and Protocols will play a significant role. The custom network protocols based on end-to- end connectivity is not suited for military communication networks, which is a long/variable delay with high error rates and greatly heterogeneous. Realization of a robust, intelligent and integrated communication and careful consideration of types of assets that have to be connected will form a solid foundation for Network Centric Warfare. The vast repertoire of military assets include Ground Troops, Armored – Non armored vehicles, Naval Platforms, Airborne units, along with Command & Control and Intelligence , Surveillance, Reconnaissance assets that may be fixed or mobile. Moreover the tactical environment is extremely harsh and with marching troops to supersonic tactical aircraft, the huge extent of mobility gap and heterogeneous nature introduces more challenges in traditional protocol design. These conditions results in Intermittent Connectivity with wide ranging communication delays.

DTN overcomes the problems associated with intermittent connectivity, long delays and high error rates using Store and Forward Message switching, caching of in – transit data packets, and message ferrying and network connection state hibernation for subsequent reactivation. Studies conducted at Intel & Berkley (Demmer 2004) have indicated significant improvement when DTN techniques are employed.

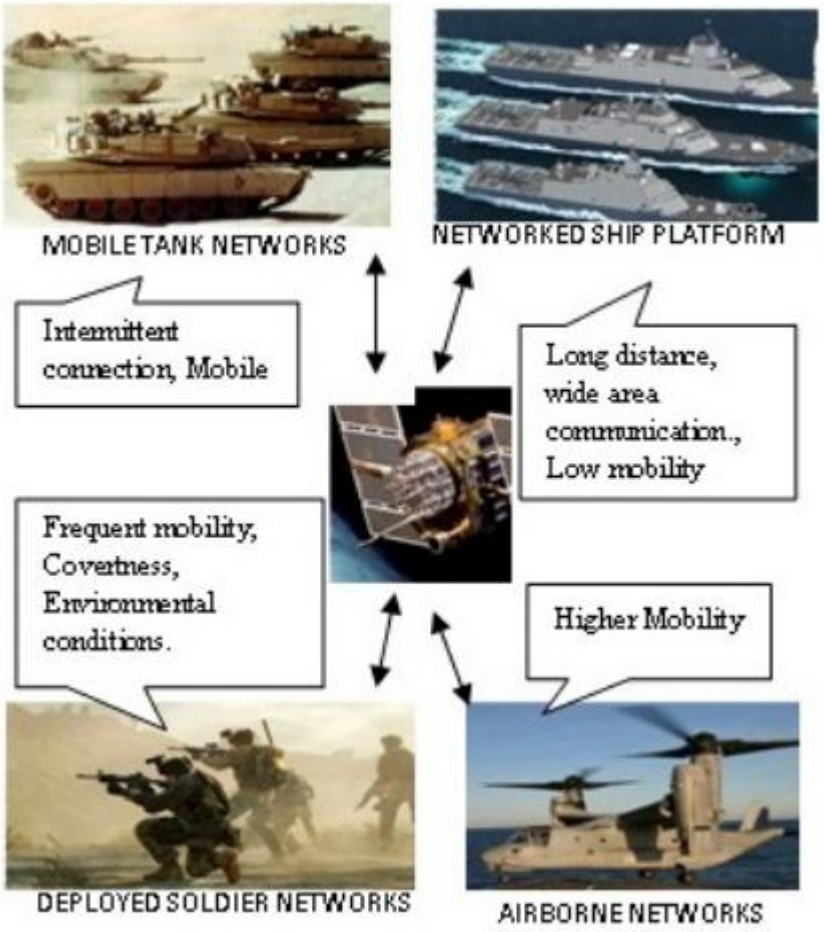


Fig 2.4: Challenges Faced In Tactical Military Operation

2.6.3 Underwater/Acoustic Networking:

The underwater acoustic networks are generally formed by acoustically connected ocean-bottom Sensors, autonomous underwater vehicles & surface stations which provide links to on – shore control centre. Underwater Acoustic network is growing rapidly due to its advantages in disaster Prevention, Harbour Portal, Underwater Robotics, Tactical under sea Surveillance, oil – gas pipelines monitoring, Offshore explorations, Pollution monitoring & oceanographic data collection, Salinity Monitoring. But the challenges include slow propagation of acoustic waves, limited bandwidth and very high delays. Multiple unmanned or autonomous underwater vehicles (UUVs, AUVs), equipped with underwater sensors, will also find its application in exploration of natural undersea resources and gathering of scientific data in collaborative monitoring missions. To make

these applications viable, there is a need to enable underwater communications among underwater devices [7]. Approaches like Delay Tolerant Network may be a better match to many underwater networks by avoiding end – to – end retransmission & supporting very sparse & often disconnected networks [8].

2.6.4 Smartphone Application:

The Delay Tolerant Network Approach can be implemented in the Android platform to provide connectivity in environments that lack Efficient Network Infrastructures. The implementation of DTN services and protocol stack on the Android platform is known as "Bytewalla" which allows the use of android phones for the physical transport of data between network nodes in areas where there are no other links available or when the existing links are highly intermittent [9].

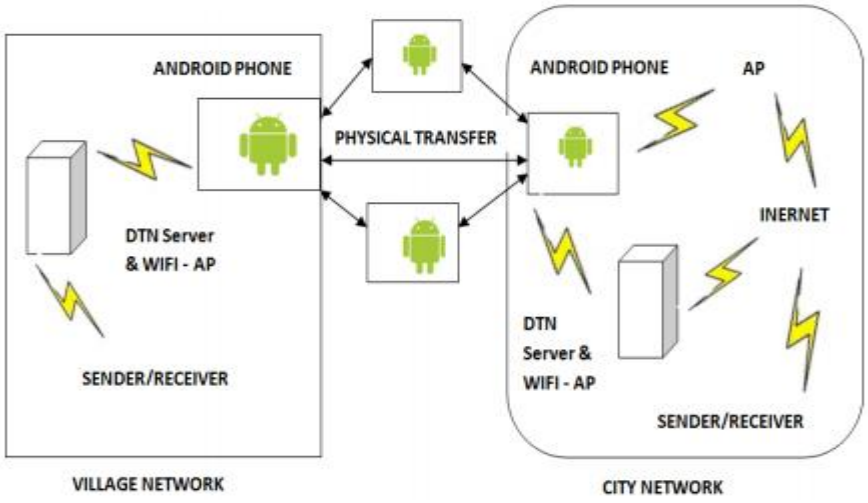


Fig 2.5: Bytewalla Architecture

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 [10]. 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.

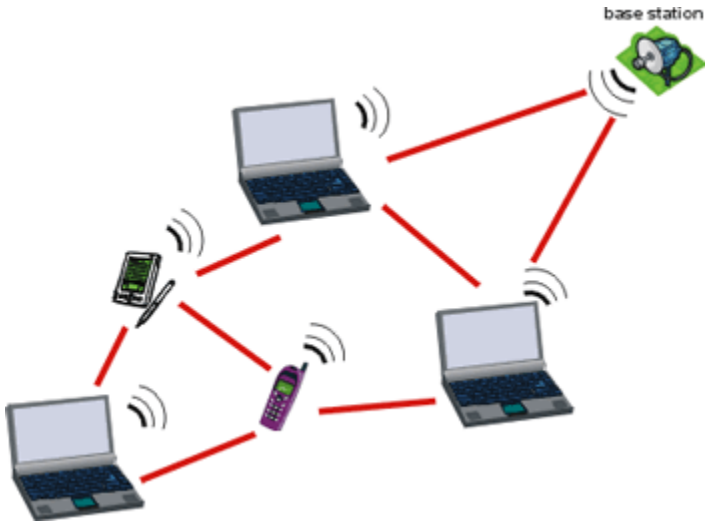


Fig 3.1: Ad-Hoc Network

An ad hoc network typically refers to any set of networks where all devices have equal status on a network 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 [11] and practical [12] 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 Characteristic 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 [13].

3.2 Ad Hoc Network Applications:

Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately that is, their applications do not interact. Imagine, however, if they could inter-act directly: participants at a meeting could share documents or presentations; business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuter exit a train, their laptops could remain online; likewise, incoming e-mail could now be diverted to their PDAs; finally, as they enter the office, all communication could automatically be routed through the wireless corporate campus network. These examples of spontaneous, ad hoc wireless communication between devices might be loosely defined as a scheme, often referred to as ad hoc networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure. Actually, ad hoc networking as such is not new, but the setting, usage and players are. 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!

Why so slow a progress in the development and deployment of commercial ad hoc applications? Main reason is that the original applications scenarios were NOT directed to mass users. 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).

Another important area that has propelled the ad hoc concept is sensor nets. Sensor nets combine transport and processing and amplify the need for low energy operation, low form factor and low cost - so, these are specialized ad hoc solutions. Nevertheless, they represent a very important growing market. In the sequel we elaborate on two applications, the battlefield and the urban and Campus grid [13].

3.2.1 The Urban and Campus Grids:

In this section we describe two sample applications that illustrate the research challenges and the potential power of ad hoc as opportunistic extension of the wireless infrastructure.

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. The emerging technologies however, will soon stimulate an explosion of new applications. Within the car, short range wireless communications (e.g., PAN technology) will be used for monitoring and controlling the vehicle's mechanical components as well as for connecting the driver's headset to the cellular phone. Another set of innovative applications stems from communications with other cars on the road. The potential applications include road safety messages, coordinated navigation, network video games, and other peer-to-peer interactions. These network needs can be efficiently supported by an "opportunistic" multi hop wireless network among cars which spans the urban road grid and which extends to intercity highways. This ad hoc network can alleviate the overload of the fixed wireless infrastructures (3G and hotspot networks). It can also offer an emergency backup in case of massive fixed infrastructure failure (e.g., terrorist attack, act of war, natural or industrial disaster, etc). The coupling of car multi hop network, on-board PAN and cellular wireless infrastructure represents a good example of hybrid wireless network aimed at cost savings, performance improvements and enhanced resilience to failures.

In the above application the vehicle is a communications hub where the extensive resources of the fixed radio infrastructure and the highly mobile ad hoc radio capabilities meet to provide the necessary services. New networking and radio technologies are needed when operations occur in the "extreme" conditions, namely, extreme mobility (radio and networking), strict delay attributes for safety applications (networking and radio), flexible resource management and reliability (adaptive networks), and extreme throughput (radios). Extremely flexible radio implementations are needed to realize this goal. Moreover, cross layer adaptation is necessary to explore the tradeoffs between transmission rate, reliability, and error control in these environments and to allow the network to gradually adapt as the channel and the application behaviors are better appraised through measurements. Another interesting scenario is the Campus, where the term "Campus" here takes the more general meaning of a place where people congregate for various cultural and social (possibly group) activities, thus including Amusement Park, Industrial Campus, Shopping Mall, etc. On a typical Campus today wireless LAN access points in shops, hallways, street crossings, etc., enable nomadic access to the Internet from various portable devices (e.g., laptops, notebooks, PDAs, etc.). However, not all areas of a Campus or

Mall are covered by department/shop wireless LANs. Thus, other wireless media (e.g., GPRS, 1xRTT, 3G) may become useful to fill the gaps. There is a clear opportunity for multiple interfaces or agile radios that can automatically connect to the best available service. The Campus will also be ideal environment where group networking will emerge. For example, on a University Campus students will form small workgroups to exchange files and to share presentations, results, etc. In an Amusement Park groups of young visitors will interconnect to play network games, etc. Their parents will network to exchange photo shots and video clips. To satisfy this type of close range networking applications, Personal Area Networks such as Bluetooth and IEEE 802.15 may be brought into the picture. Finally, "opportunistic" ad hoc networking will become a cost-effective alternative to extend the coverage of access points [13].

3.2.2 The Battlefield:

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. 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. Littoral missions are expected to be highly dynamic and unpredictable. Communication interruption and delay are likely, and active deception and jamming are anticipated.

The Office of Naval Research (ONR) is currently investigating efficient sys-tem solutions to address the above problems. ONR envisions unmanned systems of Intelligent, Autonomous Networked Agents (AINS) to have a profound influence on future naval operations allowing continuous forward yet unobtrusive presence and the capability to influence events ashore as required. Unmanned vehicles have proven to be valuable in gathering tactical intelligence by surveillance of the battlefield. For example, UAVs such as Predator and Global Hawk are rapidly becoming integral part of military surveillance and reconnaissance operations. The goal is to expand the UAV operational capabilities to include not only surveillance and reconnaissance, but also strike and support mission (e.g., command, control, and communications in the battle space). This new class of autonomous vehicles is foreseen as being intelligent, collaborative, recoverable, and highly maneuverable in support of future naval operations.

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". In such a large scale scenario the wireless, ad hoc communications among the teams are supported by a global network infrastructure (the "Internet in the sky").The global network is provisioned independently of the missions themselves, but it can opportunistically use several of the missions' assets (ground, sea or airborne) to maintain multi hop connectivity [13].

3.3 Technical Requirement for Ah-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.

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):

MANET stands for "Mobile Ad Hoc Network." A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructure-less network of mobile devices connected by wireless [14]. 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 .

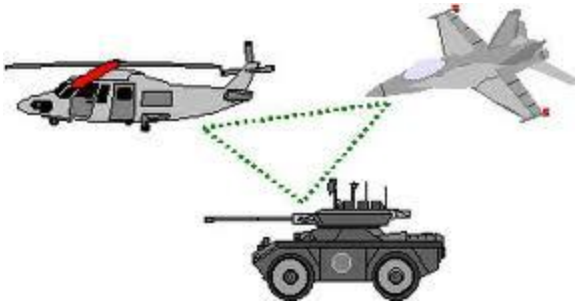


Fig 3.8: Mobile Ad-Hoc Network

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. 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.

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.

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. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc [wiki].

3.4.1 iMANET:

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.

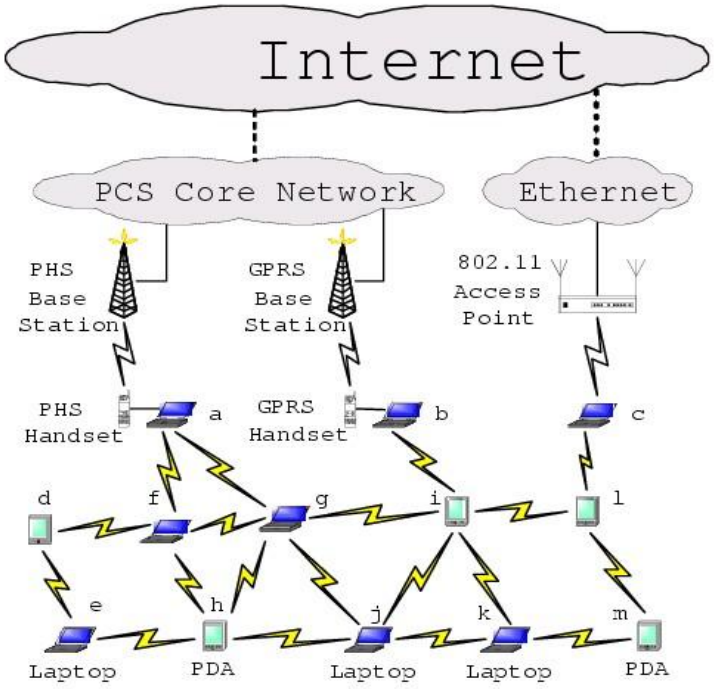


Fig 3.9: Internet Based MANET

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.

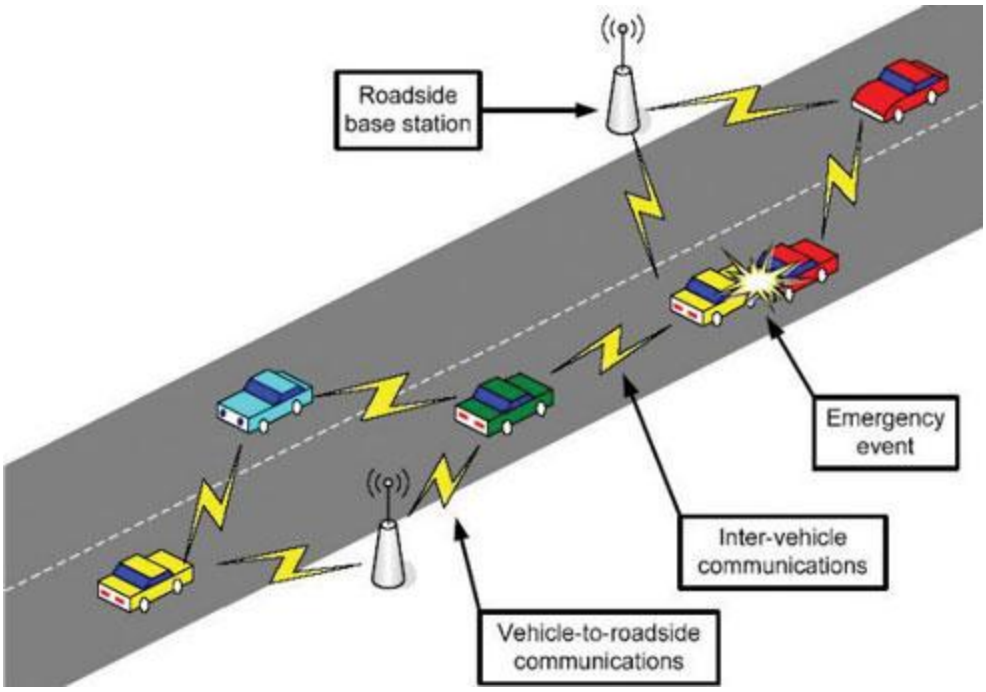


Fig 3.10: Vehicular Ad-Hoc Network (VANET)

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 Data transmission by VANET:

The main feature of VANETs is that mobile nodes are vehicles endowed with sophisticated "on-board" equipments, 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.

3.5.2 Challenges and requirements in VANET Design:

In the previous section we provide a brief review of VANET background. In reality, to successfully deploy VANET, a number of challenging issues must be addressed. 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 [15].

3.5.3 Security Challenges in VANET:

VANET poses some of the most challenging problems in wireless ad hoc and sensor network research. In addition, the issues on VANET security become more challenging due to the unique features of the network, such as high-speed mobility of network entity or vehicle, and extremely large amount of network entities. In particular, it is essential to make sure that "life-critical safety" information cannot be inserted or modified by an attacker; likewise, the system should be able to help establishing the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to other users.

In the past few years, considerable effort has been spent in research on VANET networking protocols and applications. However, research on security threats and solutions and reliability of VANET only started recently, e.g., [16-21]. Summarizing from the recent researches above, VANET security should satisfy the following requirements: message authentication and integrity, message non-repudiation, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification[15].

Message Authentication and Integrity: Message must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message. Message Non-Repudiation: The sender of a message cannot deny having sent a message [15].

Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.

Availability: The network and applications should remain operational even in the presence of faults or malicious conditions. This implies not only secure but also fault-tolerant designs, resilience to resource depletion attacks, as well as survivable protocols, which resume their normal operations after the removal of the faulty participants.

Privacy and Anonymity: Conditional privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses.

Liability Identification: Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. As part of the "conditional privacy" above, the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses. Several attacks have been identified that can be classified depending on the layer the attacker uses. At the physical and link layers the attacker can disturb the system either by jamming or overloading the channel with messages. Injecting false messages or rebroadcasting an old message is also a possible attack. The attacker can also steal or tamper with a car system OBU or destroy a roadside unit, RSU. At the network layer the attacker can inject false routing messages or overload the system with routing messages. The attacker can also compromise the privacy of drivers by revealing and tracking their positions. The same attacks can also be achieved using the application layer. In the following, we summarize the major vulnerabilities and security threats of VANET [15].

3.5.4 VANET Applications:

In the previous discussion we address the network design issue from the security perspective. In practice, a good system design also depends on understanding the applications that will be carried in the network. These applications not only call for diverse solutions, such as bandwidth, delay, security, and reliability, but also demonstrate different communication patterns, such as one-to-one, one-to-many, many-to-one, and many-to-many. However, most existing wireless network architectures could not efficiently support such demands. Therefore, 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.[15].

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. In the MAC layer, the Electronic Toll Collections application should be able to access the DSRC service channels except the control channel, with the 3rd highest priority [15]. .

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 [15].

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 [15].

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[15].

3.5.5 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).

3.5.6 InVANET:

Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

Chapter 4

Our work

4.1 Our Model Scenario:

We have considered a highway where vehicles are moving. We want 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 (e.g, sink A and sink B) at two ends can simultaneously generate and receive data. The generated data by sink A or sink B is delivered to sink B or sink A respectively by the cars.

The basic algorithm to delivery data is –"**store and carry**". Every vehicle collects data from the sink and stores it. Then it carries the data by itself and whenever it finds any other vehicle within its wi-fi range, it forwards the collected data [1]. Thus data delivery is done from one end to the other end.

Sink: There are two sinks at two ends, sink A and sink B. Each sink can generate and receive data simultaneously and the generated data is delivered by the vehicles.

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

Vehicle: We have taken car and truck as vehicles. Car and truck move in opposite direction. We assume that, every vehicle has a data storage system and a power supply that supplies power. Vehicles will always try to connect to each other within their wi-fi range. If a vehicle finds any other vehicle within its range, it will deliver the data. The new vehicle then carries the data until it finds another vehicle within its range. Thus data is stored, carried and forwarded to the sink. We also assume that the vehicles do not change their route.

Wi-fi range: Wi-fi range of each vehicle is 250 m. Within this range a vehicle can connect with other vehicles and transfer data.

Speed: We run our simulation for the speeds of 36 km/h and 72- km/h. We consider 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.

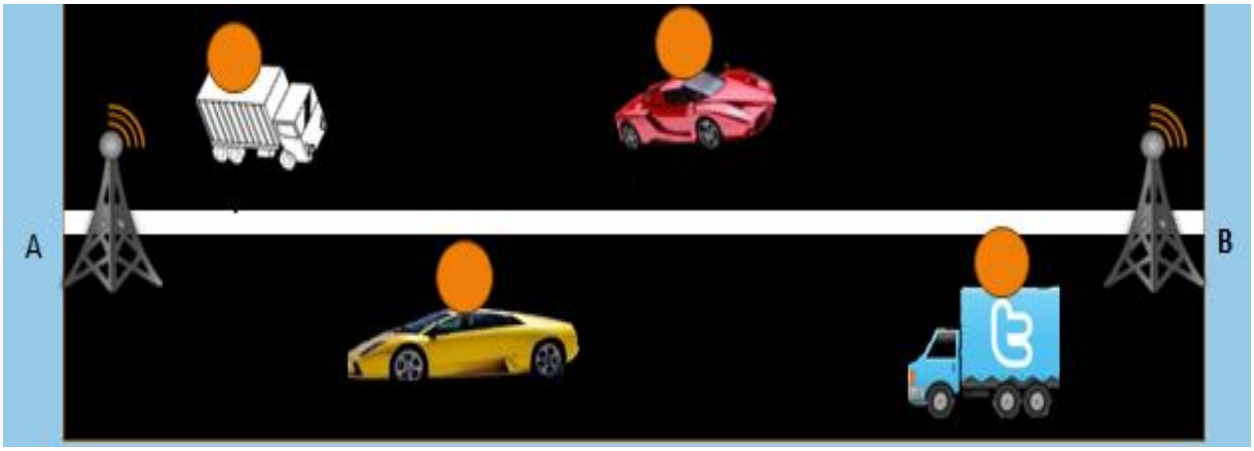


Fig 4.1: One way one direction data

In the figure (4.1), 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.

One way one direction can be useful in cases where there are issues of 'data security'. As data is not forwarded to other vehicles, the other vehicles do not have access to the data. Suppose a company have two or more branches and there are regular exchanges of goods between these branches via truck. This truck can be used to convey any transactional or any other company policy related information. Certainly the company is not going to expose this information to other companies. In this case one way one direction is suitable.

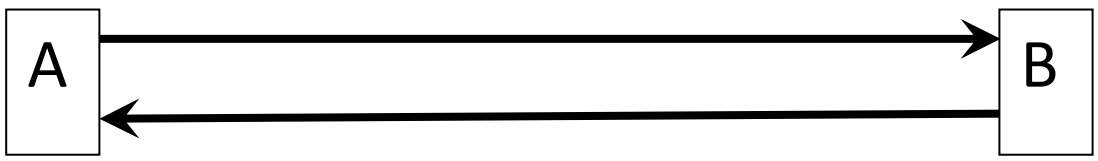
Another case may involve connecting two EPZ's (in Bangladesh). Everyday hundreds of vehicles are carrying products between the Savar EPZ and Chittagong EPZ. So a data network can be easily established using this vehicle. And if there is any confidential information needs to be delivered then one way one direction can be used. Government vehicles carrying sensitive information can also use one way one direction scheme.

In one way one direction every vehicle carries its own data. So data delivery rate can be lower and there is less chance of data loss or data duplication as there is no hopping of data into the next vehicle.

4.2.2 Multi-Hop One Direction:

Multi-hop one direction is the second scheme for transferring data from one place to another. It is a slight modification of one way one direction. Unlike one way one direction, here data hops from vehicle to vehicle. 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 it's 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).

The direction of data does not change here also. Data flows from either point A to point B or from point B to point A. So there is hopping between the vehicles of same direction but there is no hopping between the vehicles of opposite direction.



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.

In multi-hop one direction, one thing to remember that, always a data is forwarded to a vehicle that is ahead of it. No data is hopped to a vehicle that is behind it.

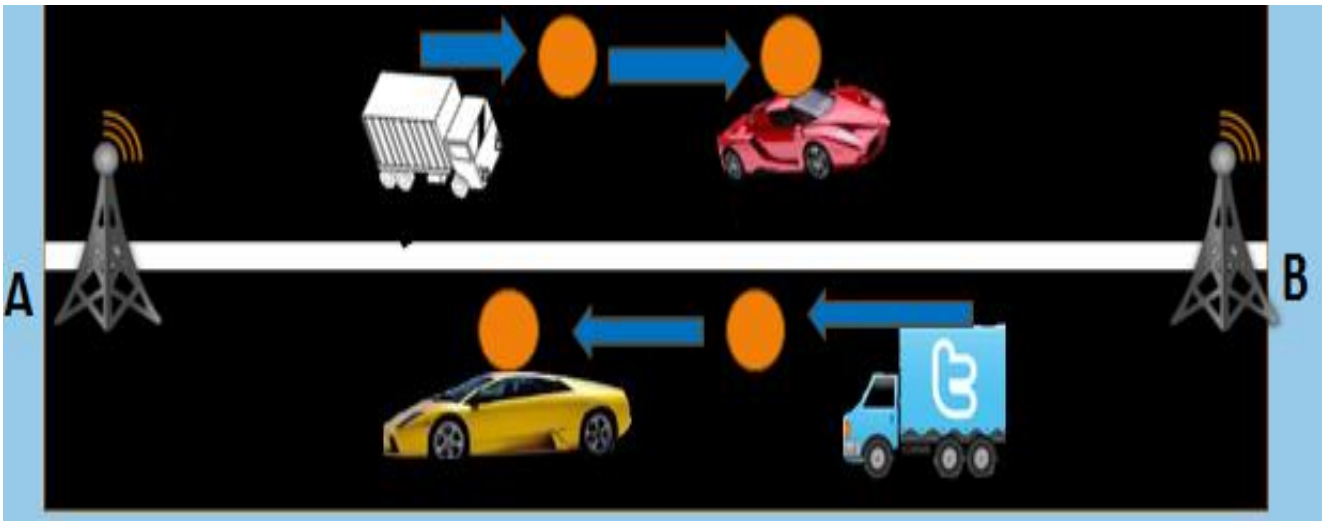


Fig 4.2: Multi-hop one direction

Here (figure 4.2) 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.

For this scheme every vehicle must have sufficient storage so that all data coming from other vehicles can be stored. Data delivery rate significantly improves because of data hopping. When vehicle density increases then hopping increases as more vehicles get connected with one another.

4.2.3 Multi-Hop Multi-Direction:

Multi-hop multi-direction is the last of the three schemes for delivering data. It is similar to multi-hop one direction but with a new feature. 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.

In multi-hop multi-direction every vehicle receives data from the sink and move towards the destination. 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.

Anyway, data is being forwarded in such a way that data travels along the shortest path between the source and destination. The links between the vehicles of both directions are established in a way that ensures the shortest path between the source sink and destination sink.

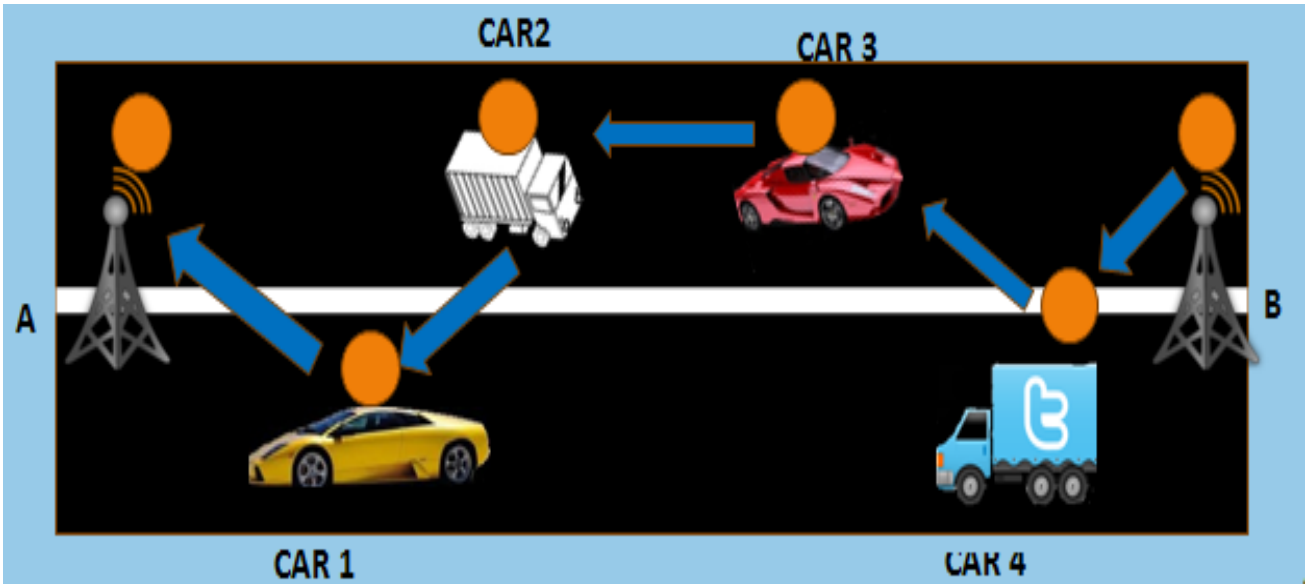


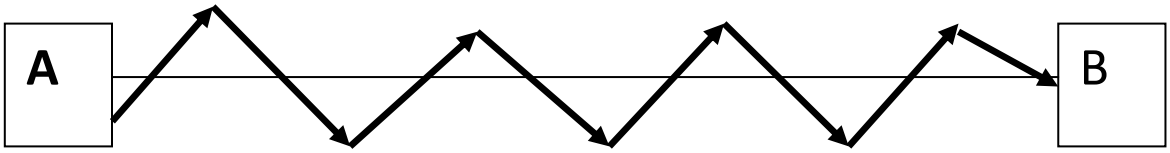
Fig 4.3: Multi-hop multi-direction

From the above figure (4.3) we see that there are four vehicles –car1, car2, car3 and car4. Car1 and car4 are moving from sink B to sink A whereas car2 and car 3 are moving from sink A to sink B.

Suppose sink B wants to send some data to sink A. 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. But in case of multi-hop multi-direction car4 can connect with car 3 which is a vehicle of opposite direction and hops the data to car 3. Car3 again hops the data to car car2 which is a vehicle of same direction and which is behind car3. Car 2 finally hops the data to car 1 which is in the original direction of the data and car 1 delivers the data to sink A.

Here data direction changes frequently according to availability of vehicles. Data delivery rate is faster than the previous two schemes as data is delivered through the shortest path.

A typical data direction diagram of multi-hop multi-direction can be:



4.3 Simulation:

For simulation we used "**NetLogo**" 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 300 data and delivers it to the other sink. That means sink A generates 300 data which is delivered to sink B via all the three schemes one way one direction, multi-hop one direction, multi-hop multi-direction separately. We considered 30 vehicles in 5kilometerof road length. 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 and we chose two different speeds of 36 km per hour and 72 km per hour.

No	Parameter	Value
1	Length of the road	5 kilometers
2	Number of data (for a single sink)	300
3	Speed of the vehicle	36 km/h and 72km/h
4	Number of vehicle	30
5	Wi-fi range	250 meter

Table 4.1: Simulation Setup

We ran our simulation on a platform (pc) 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	Default System BIOS
7.	Processor	Intel(R) Core(TM)2 Quad CPUQ8400 @ 2.66GHz (4 CPUs), ~2.7GHz
8.	Memory	4096MB RAM
9.	Available OS Memory	4062MB RAM
10.	Page File	1159MB used, 6961MB available
11.	Windows Dir	C:\Windows
12.	DirectX Version	DirectX 11
13.	DX Setup Parameters	Not found
14.	User DPI Setting	Using System DPI
15.	System DPI Setting	96 DPI (100 percent)
16.	DWM DPI Scaling	Disabled
17.	DxDiag Version	6.01.7600.16385 32bit Unicode

Table 4.2: system Configuration

Chapter 5

Results and Discussion

As mentioned before, we ran our simulation for road length of 5 km and vehicle speed was chosen to be 36 km/h and 72 km/h. For total data of 600 we found the following data:

Name of the scheme	Number of received data by Sink1	Number of received data by Sink2	Total received data	Received time (sec) Sink 1	Received time (sec) Sink 2	Total received time (sec)	Average data delivery rate (data/sec)
One way one direction	300	300	600	723.668	734.684	1458.352	**0.4114**
Multi-hop one direction	300	300	600	707.08	714.105	1421.185	**0.4221**
Multi-hop multi-direction	300	300	600	481.317	481.083	962.4	**0.6234**

Table 5.1: data collection for speed 36 km/h and road length 5 km

From the table 5.1, we found that data delivery rate (**0.6234** data/sec) is highest for multi-hop multi-direction and lowest (**0.4114** data/sec) or one way one direction. It is easily understandable because in multi-hop multi-direction data was delivered using the shortest path whereas in one way one direction every vehicle carried its own data to the destination. Data delivery rate in multi-hop one direction is on between one way one direction and multi-hop multi-direction.

Name of the scheme	Number of received data by Sink1	Number of received data by Sink2	Total received data	Received time (sec) Sink 1	Received time (sec) Sink 2	Total received time (sec)	Average data delivery rate (data/sec)
One way one direction	300	300	600	418.445	424.454	842.899	**0.7118**
Multi-hop one direction	300	300	600	344.811	349.763	694.574	**0.8638**
Multi-hop multi-direction	300	300	600	253.154	253.046	506.2	**1.1853**

Table 5.2: Data collection for speed 72 km/h and road length of 5 km

Here in table 5.2, we again found that the data delivery rate is highest (**1.1853** data/sec) in multi-hop multi-direction and lowest (**0.7118** data/sec) in one way one direction. We also saw that data delivery rate increased as speed of vehicles increased.

Sink A delivered 300 data to sink B and sink B delivered 300 data to sink A.

In each case all three schemes were used and different speeds of vehicle also.

We found necessary data for all cases and we used these data to determine the suitable option for data delivery.

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

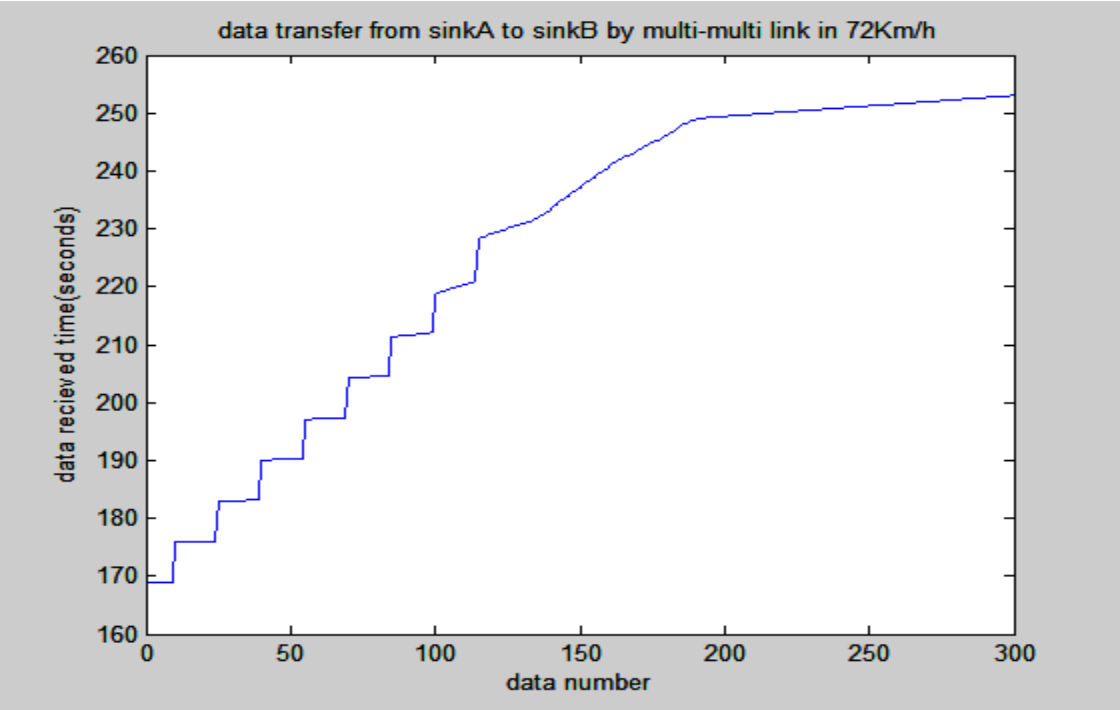


Fig 5.1: received time vs data number [72 km/h][sink A to sink B][multi-multi link]

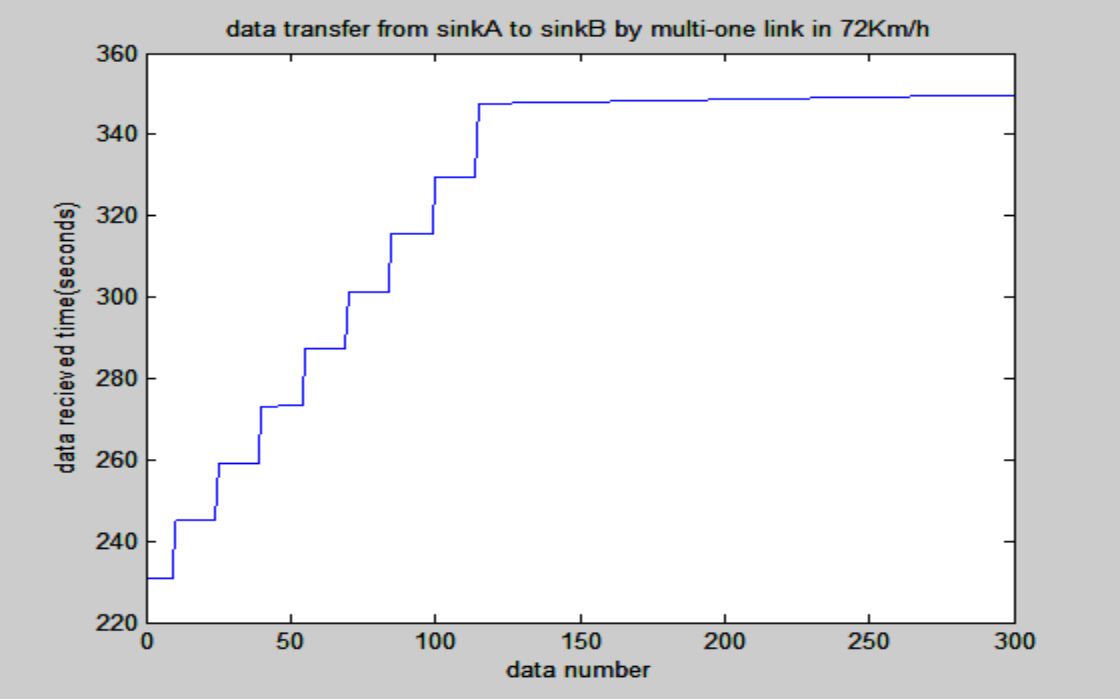


Fig 5.2: received time vs data number [72 km/h][sink A to sink B][multi-one link]

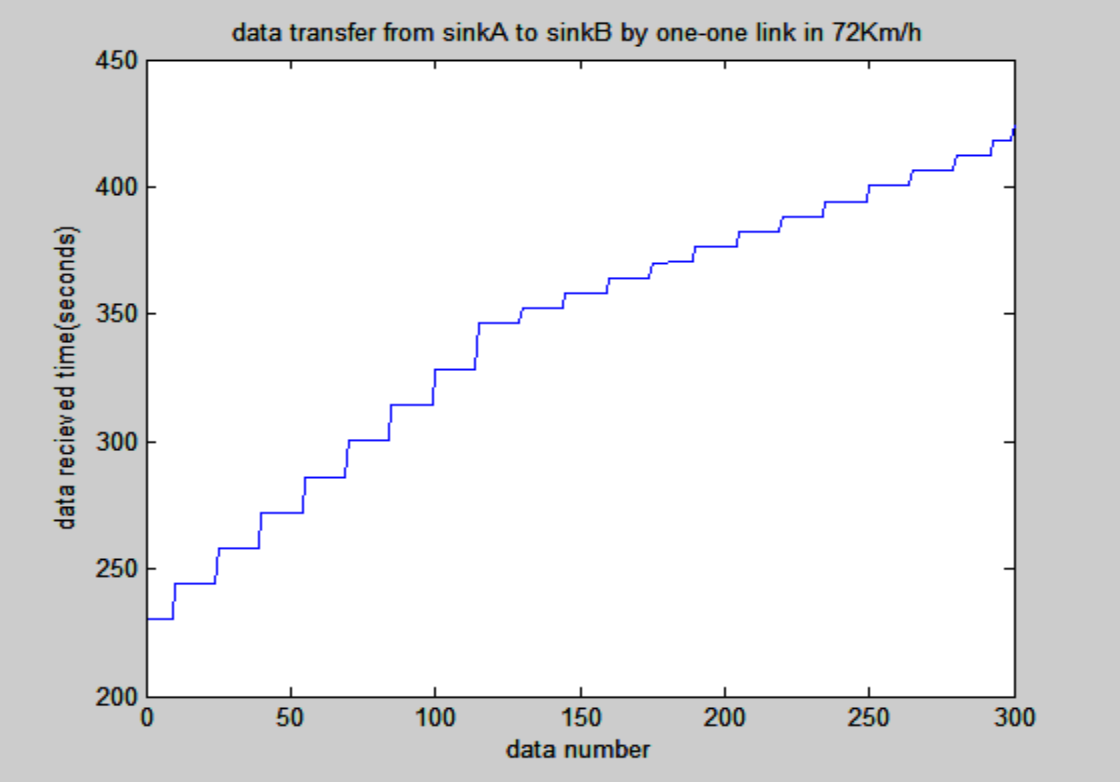


Fig 5.3: received time vs data number [72 km/h][sink A to sink B][one-one link]

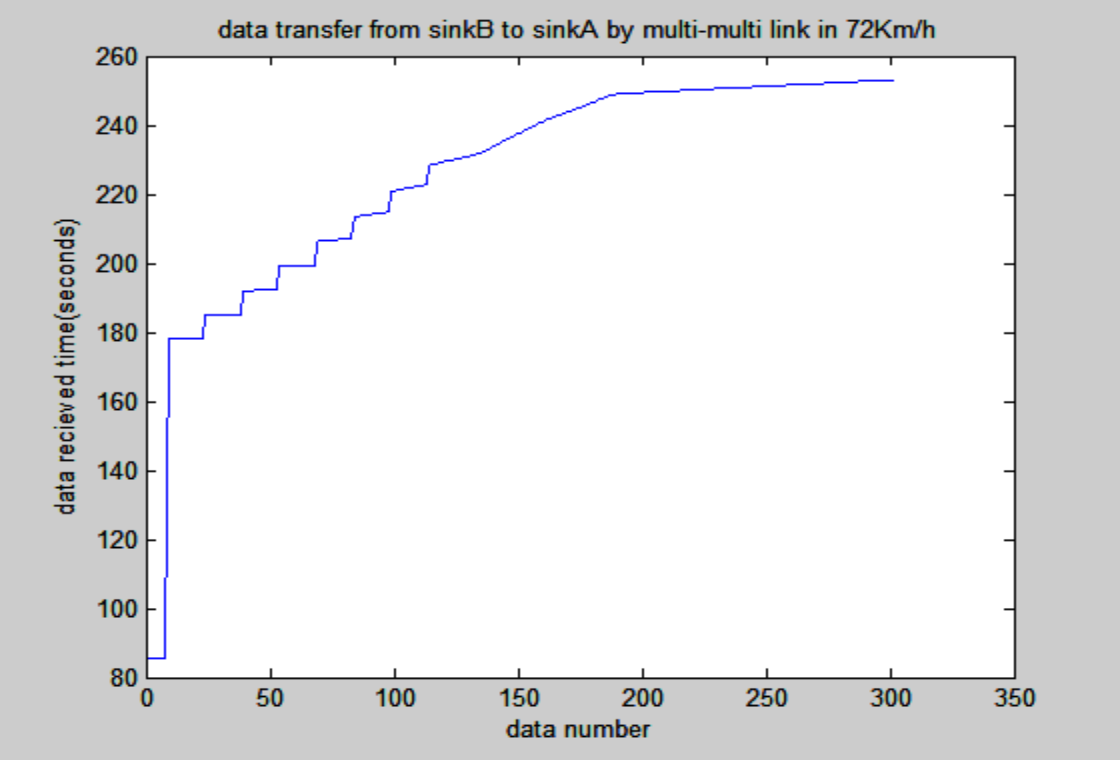


Fig 5.4: received time vs data number [72 km/h][sink B to sink A][multi-multi link]

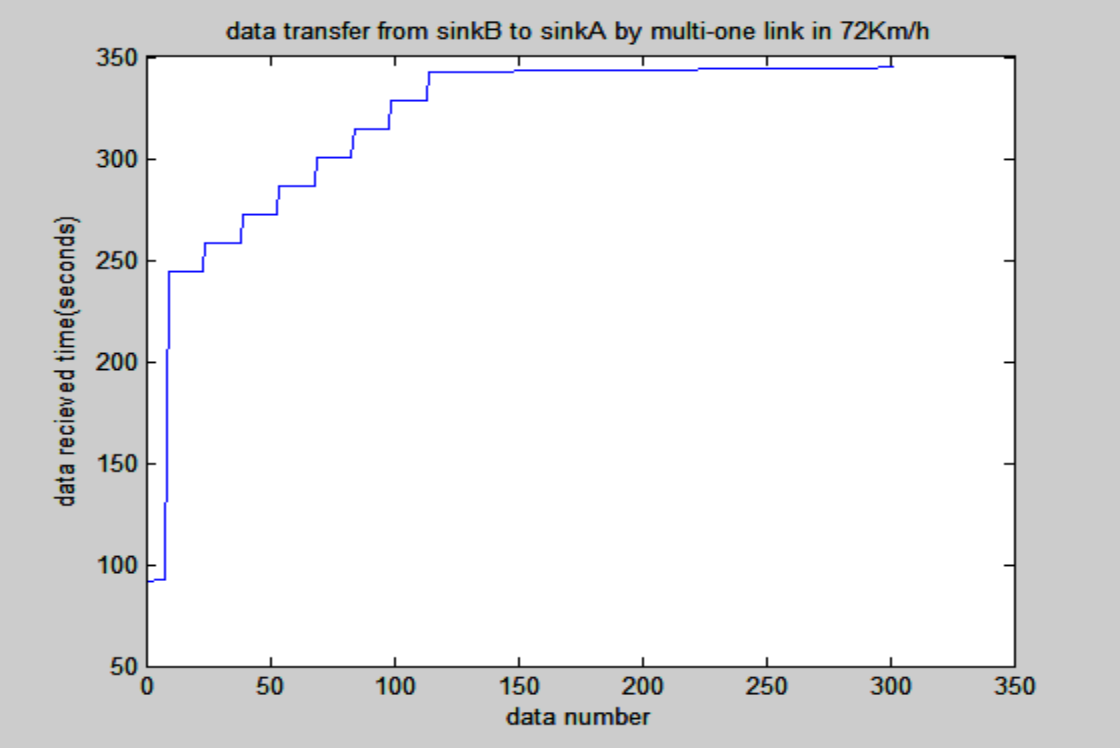


Fig 5.5: received time vs data number [72 km/h][sink B to sink A][multi-one link]

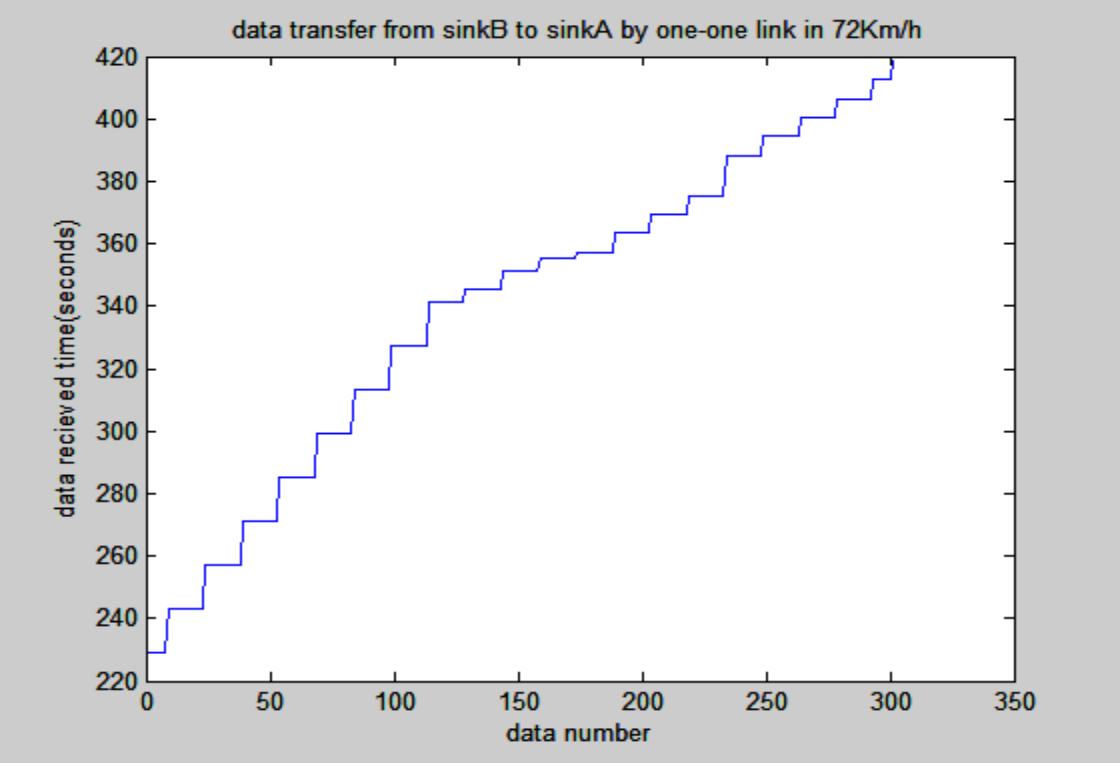


Fig 5.6: received time vs data number [72 km/h][sink B to sink A][one-one link]

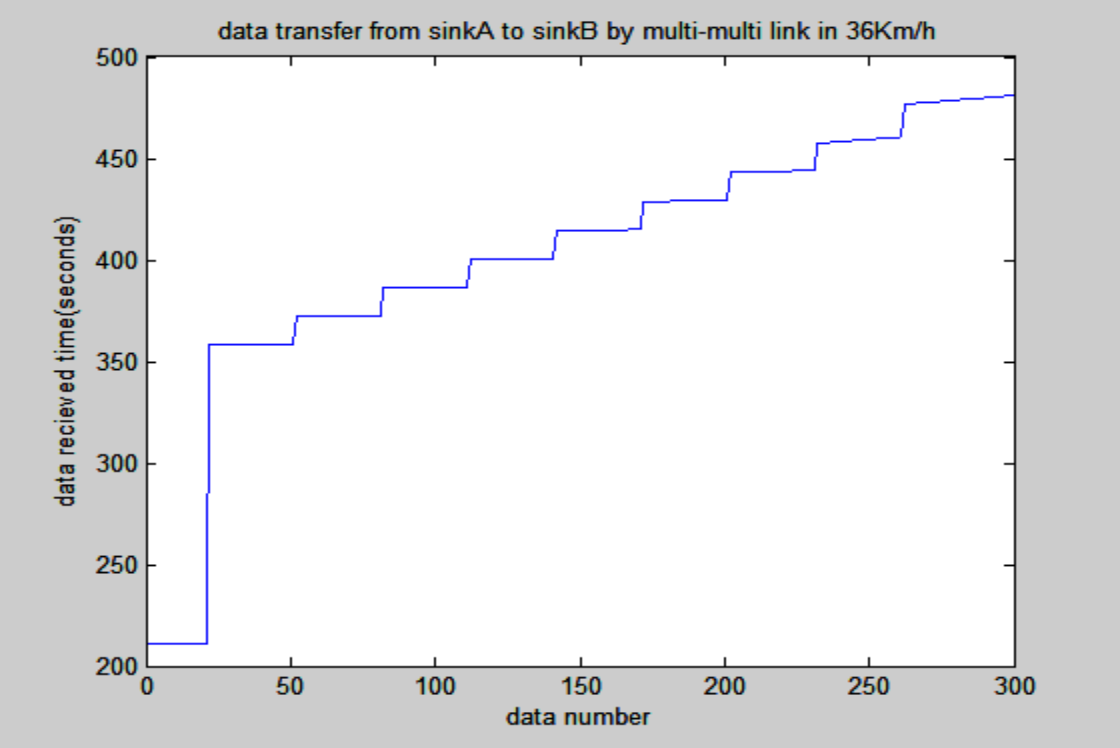


Fig 5.7: received time vs data number [36 km/h][sink A to sink B][multi-multi link]

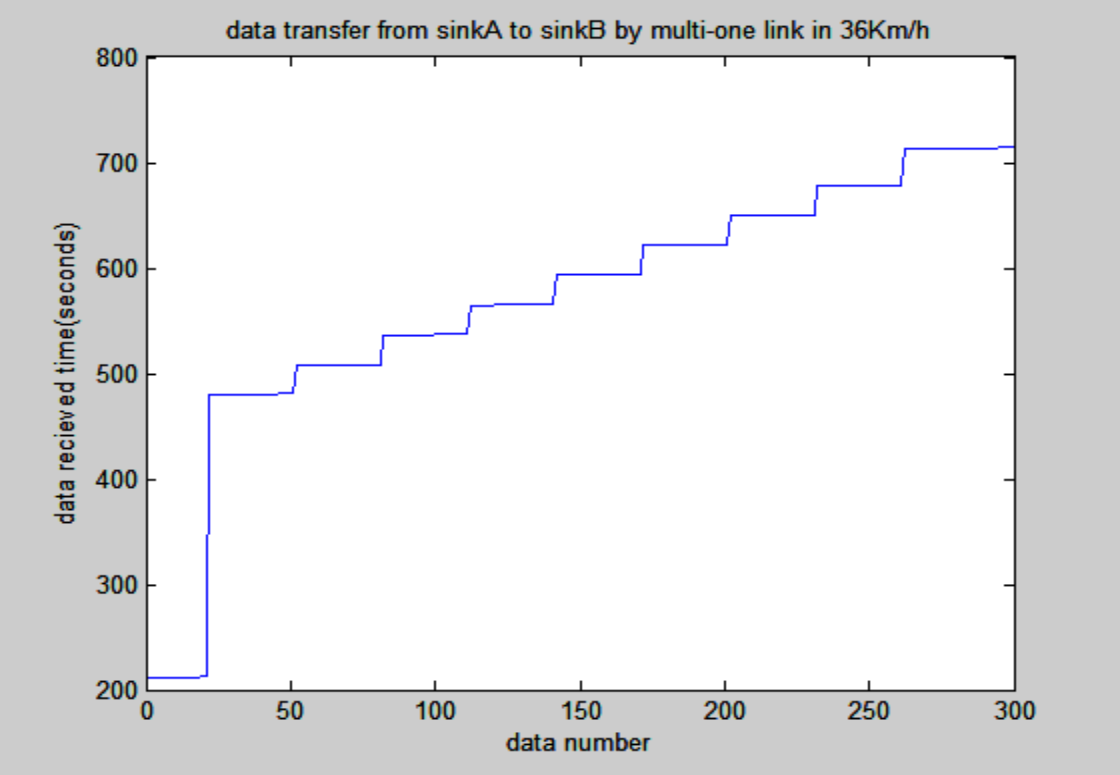


Fig 5.8: received time vs data number [36 km/h][sink A to sink B][multi-one link]

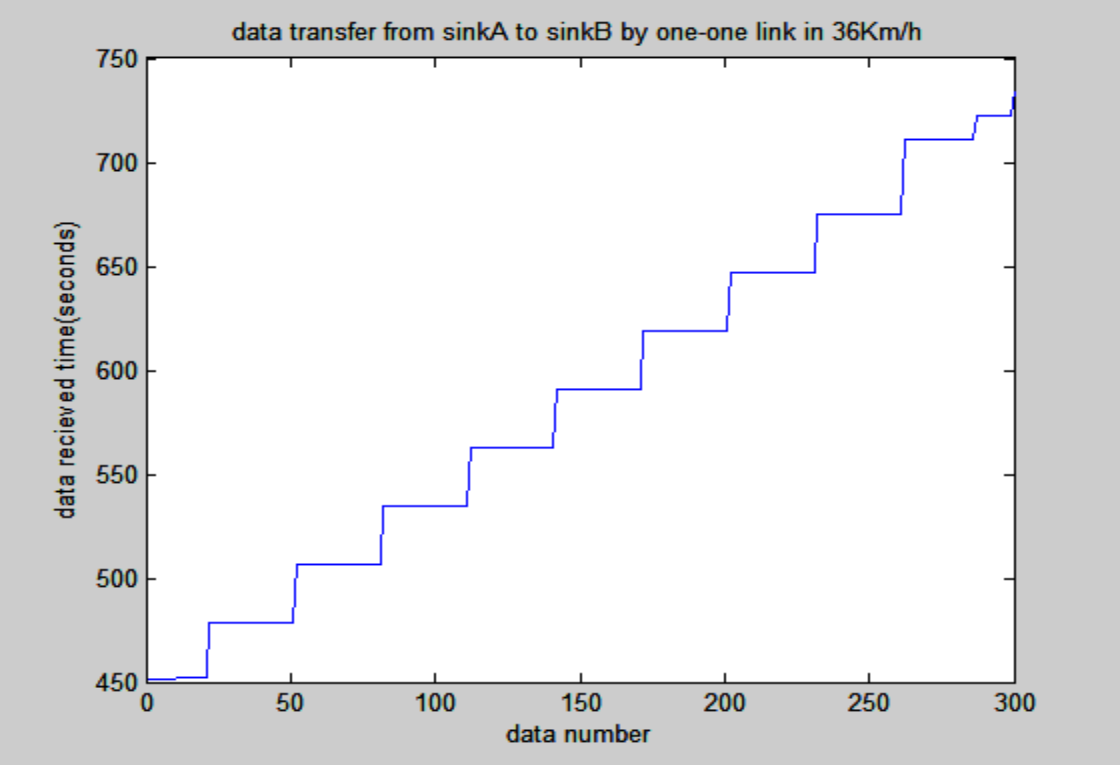


Fig 5.9: received time vs data number [36 km/h][sink A to sink B][one-one link]

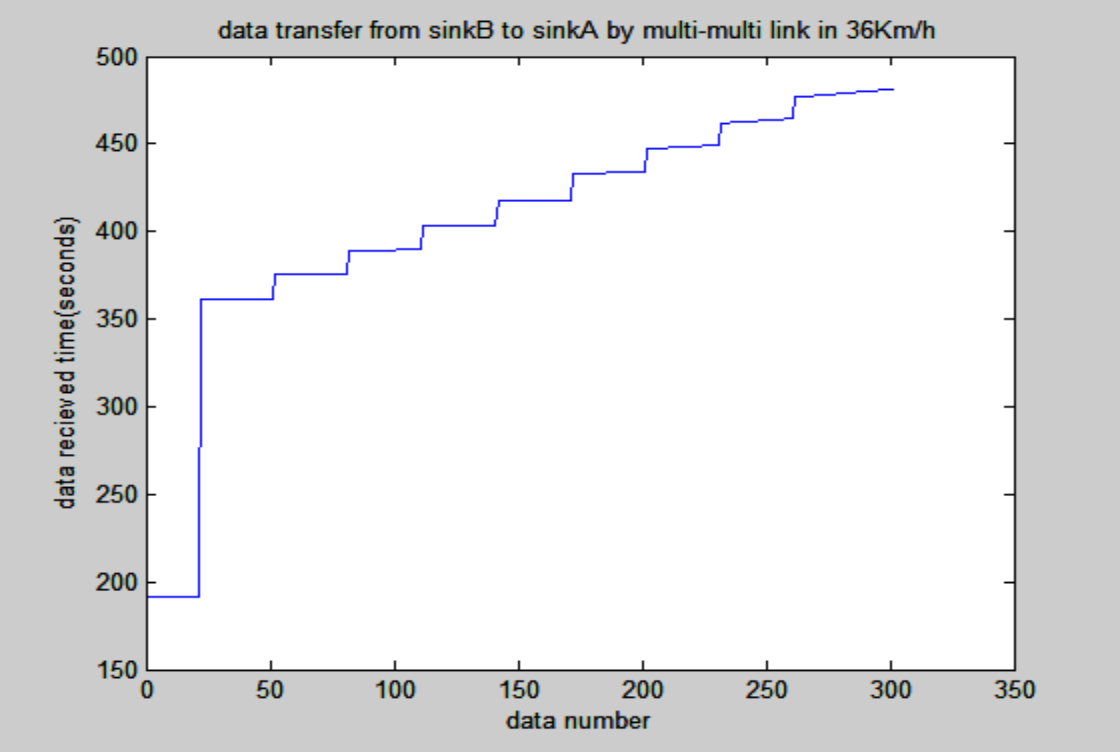


Fig 5.10: received time vs data number [36 km/h][sink B to sink A][multi-multi link]

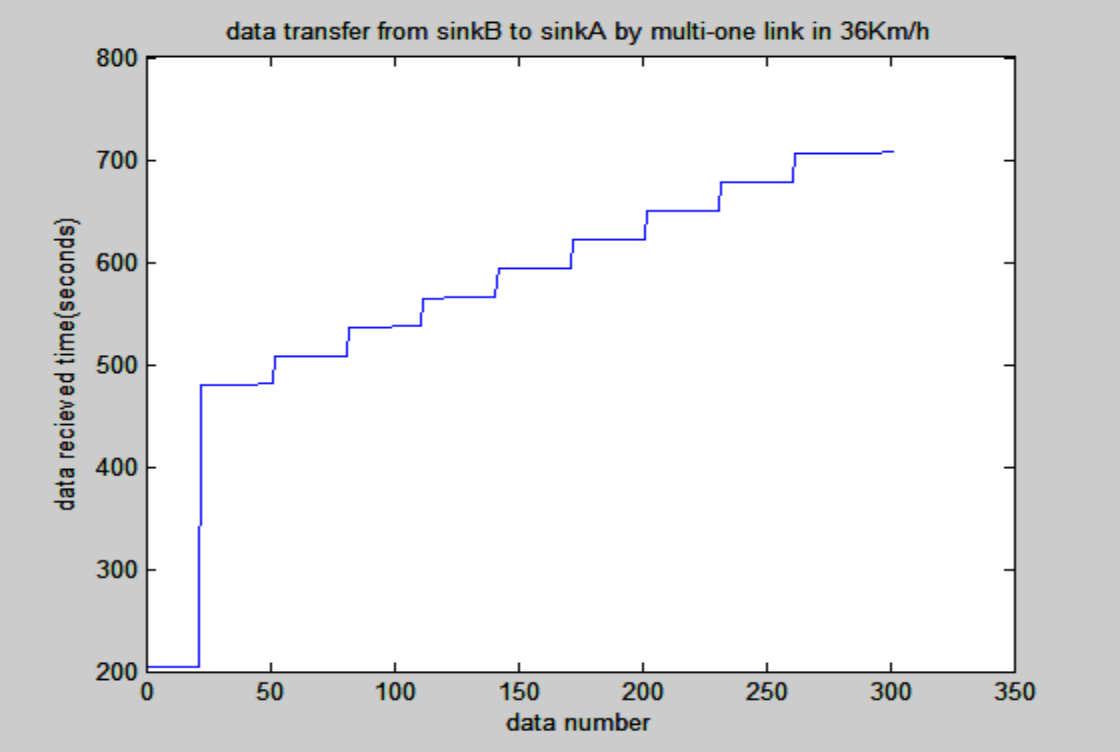


Fig 5.11: received time vs data number [36 km/h][sink B to sink A][multi-one link]

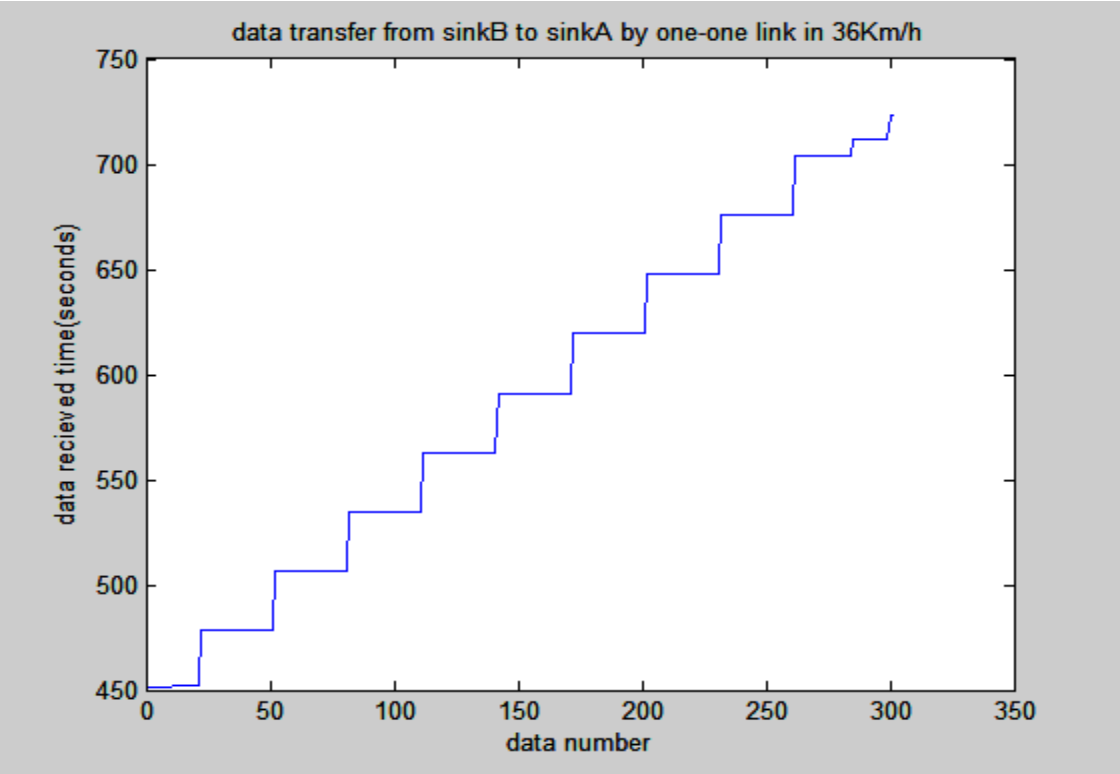


Fig 5.12: received time vs data number [36 km/h][sink B to sink A][one-one link]

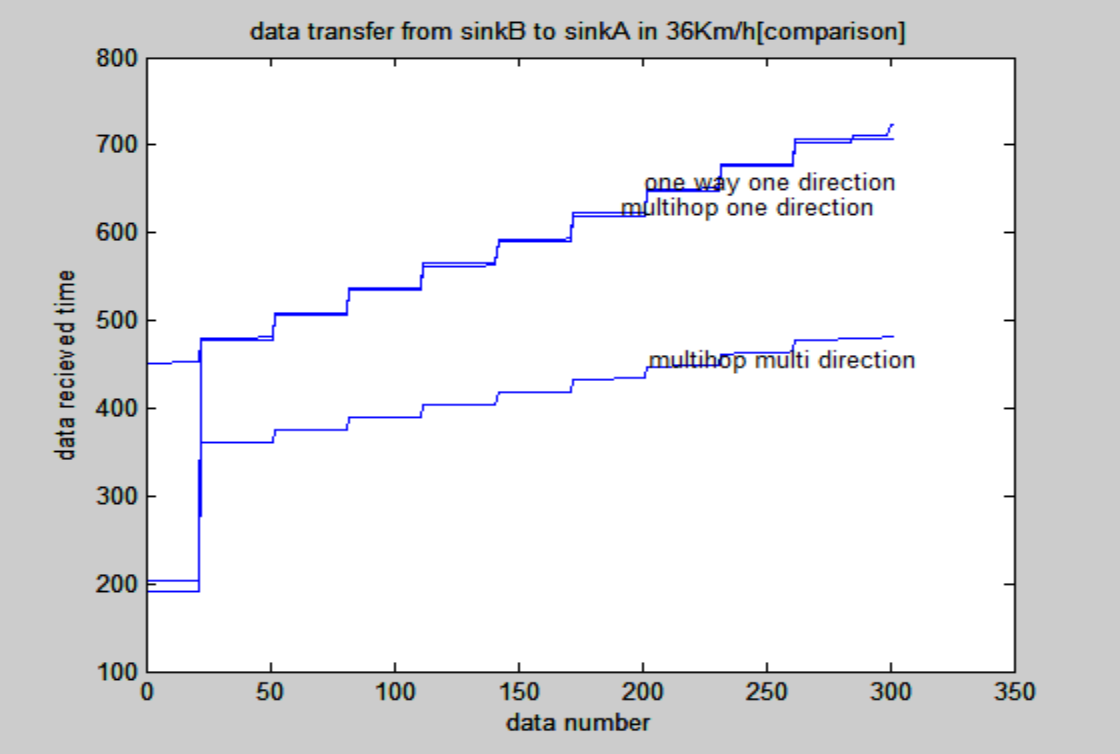


Fig 5.13: Comparison (received time vs data number) [36 km/h][sink A to sink B]

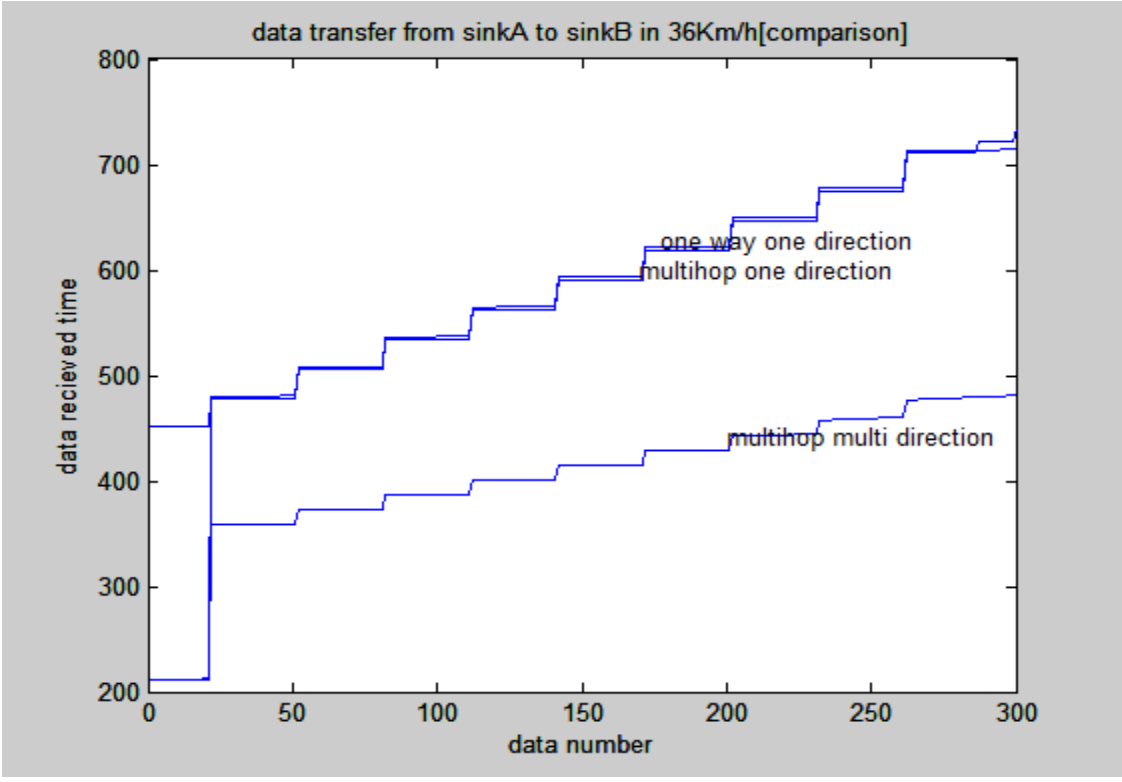


Fig 5.14: Comparison (received time vs data number) [36 km/h][sink A to sink B]

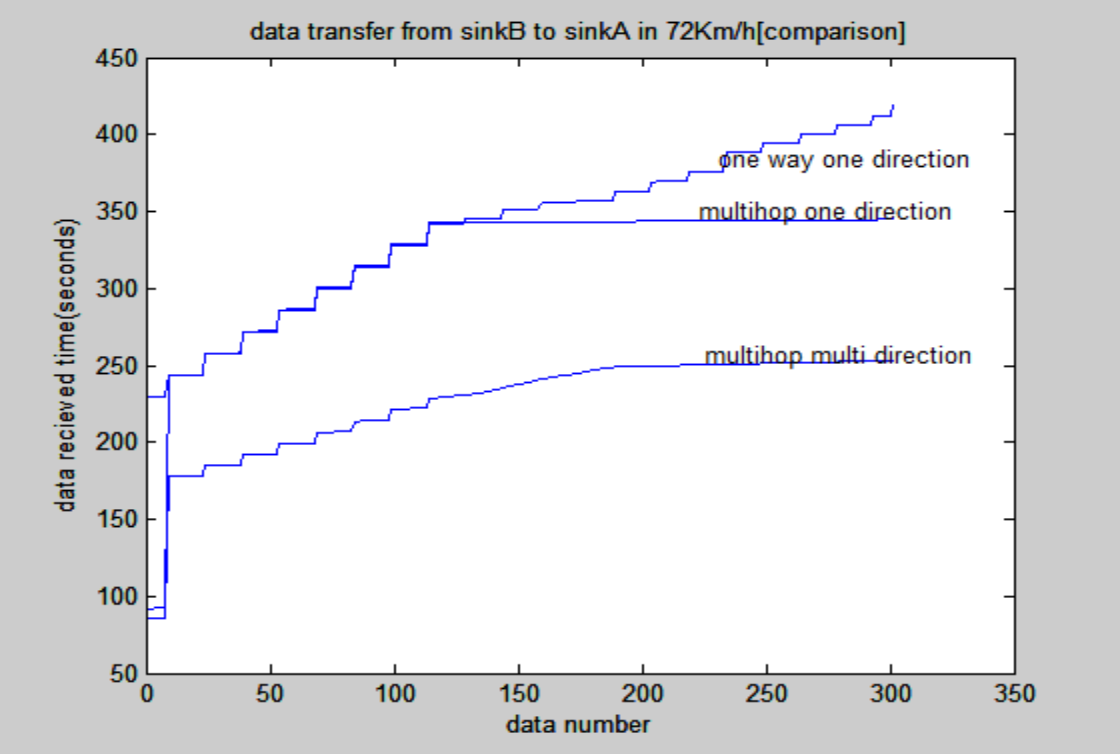


Fig 5.15: Comparison (received time vs data number) [72 km/h][sink B to sink A]

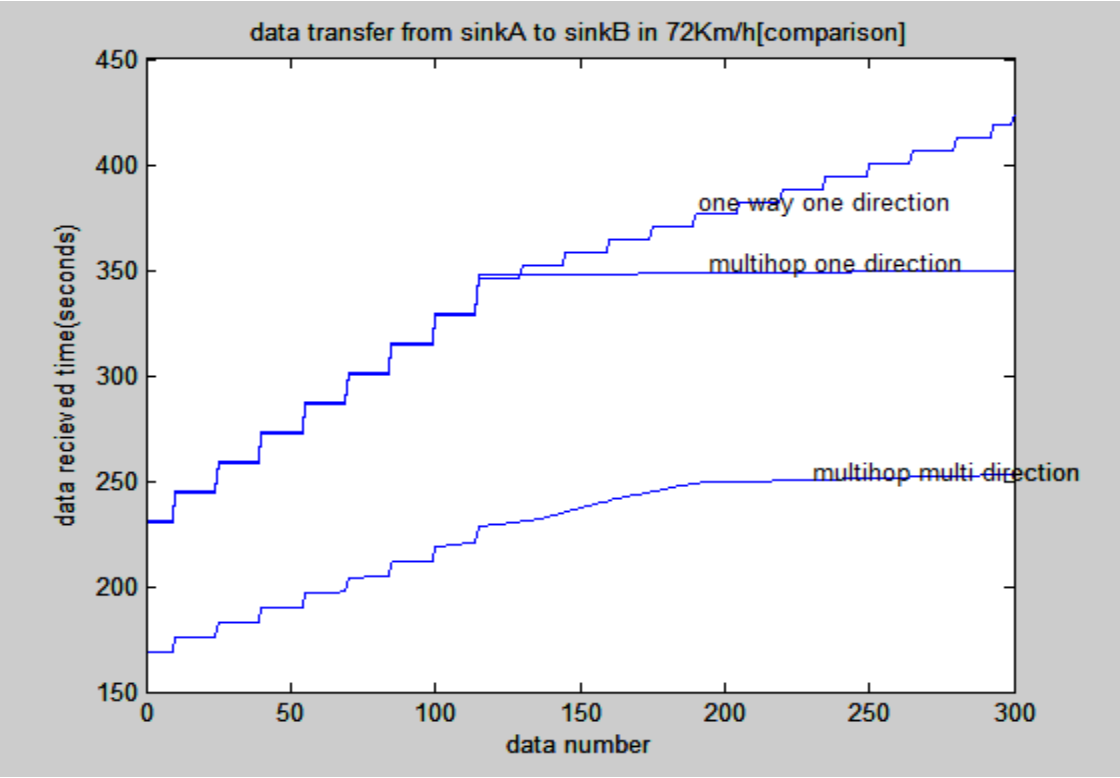


Fig 5.16: Comparison (received time vs data number) [72 km/h][sink A to sink B]

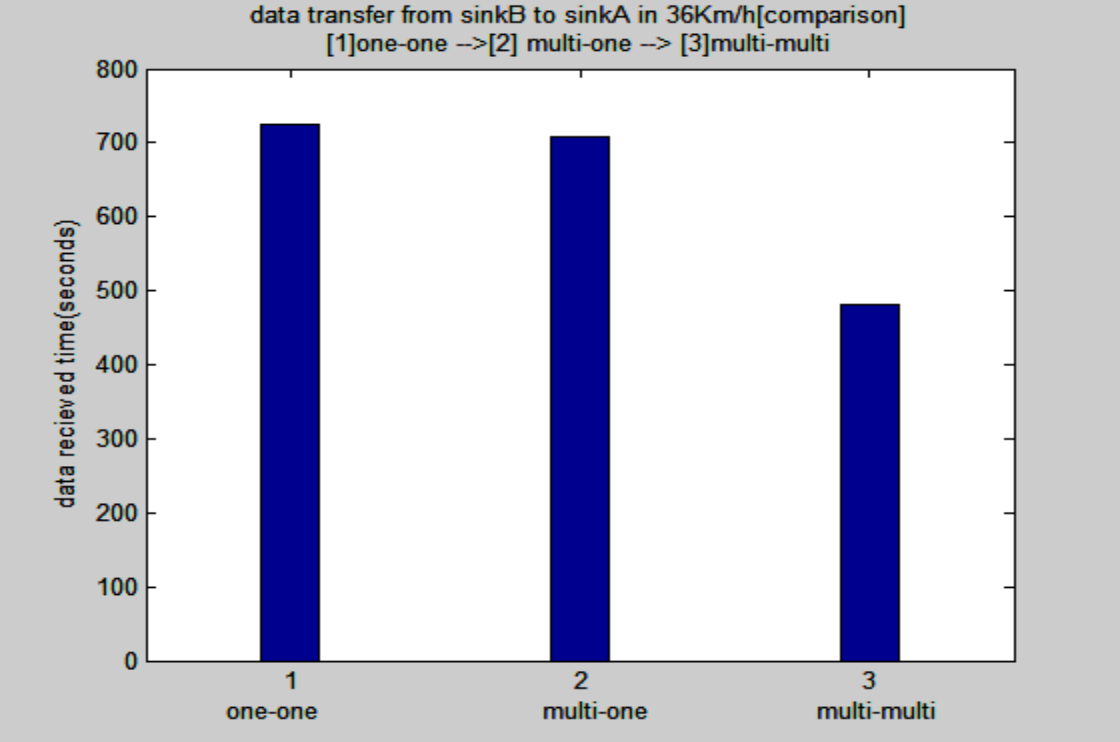


Fig 5.17: Comparison (in term of received time) [36 km/h][sink B to sink A]

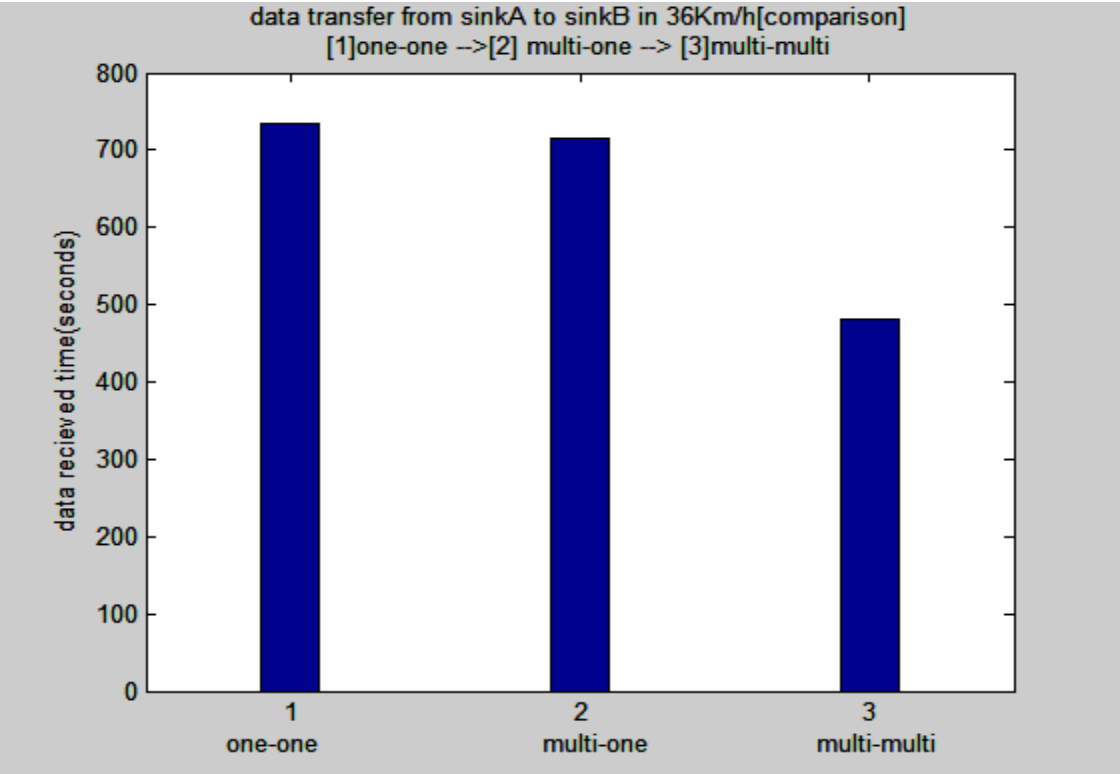


Fig 5.18: Comparison (in term of received time) [36 km/h][sink A to sink B]

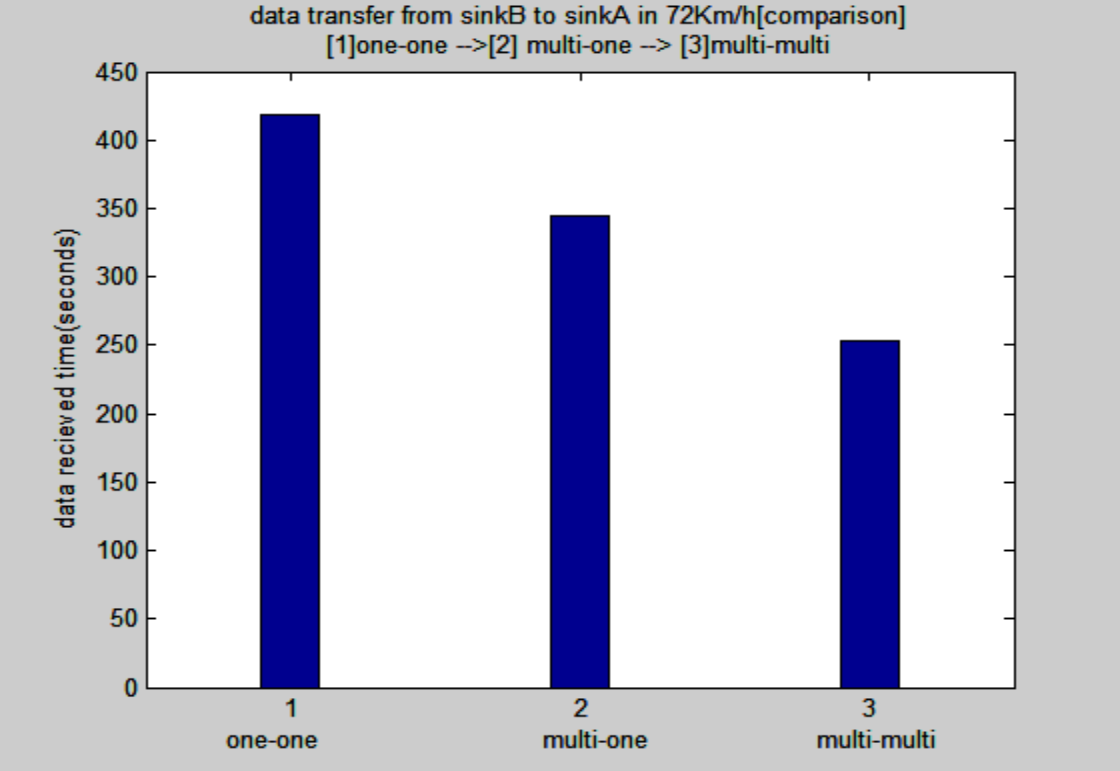


Fig 5.19: Comparison (in term of received time) [72 km/h][sink B to sink A]

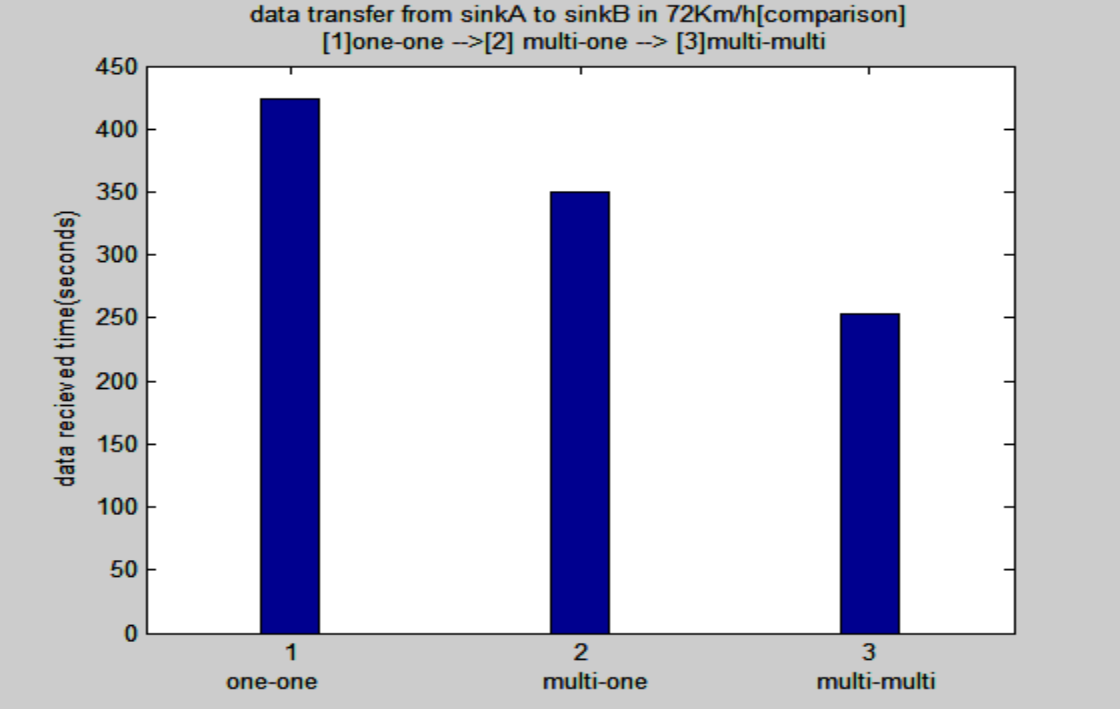


Fig 5.20: Comparison (in term of received time) [72 km/h][sink A to sink B]

Chapter 6

Conclusion

The driving force behind this dissertation was the emergence of creating a data network in infrastructure-less scenario. We saw that highways could be a suitable field to create such a network using vehicles as mobile nodes. We designed three schemes for delivering data in a vehicular network in highways. Among them multi-hop multi-direction is superior from data delivery rate point of view. One way one direction is the slowest and multi-hop one direction is moderate from the same point of view. For faster data delivery multi-hop multi-direction is suggested. One way one direction is best for securing confidentiality of the data. We found the results by extensive software simulation. We can use these findings to practically implement such networks. This requires further study on large scale to address the problems that may appear in real world such as storage capacity, power supply, noise, data loss, data duplication etc.

References

[1] A Delay-Tolerant Network Architecture for Challenged Internets, K. Fall, SIGCOMM, August 2003

[2] Artemios G. Voyiatzis, "A survey of delay – disruption tolerant networking applications", Journal of Internet

[3]. Evan P.C. Jones, Paul A.S. Ward, "Routing Strategies for Delay – Tolerant Networks", University of Waterloo, Canada.

[4] 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

[5] 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.

[6] 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.

[7] Ian F. Akyildiz , Dario Pompili, Tommaso Melodia, "Underwater acoustic sensor networks: research challenges", Published by ©Elsevier B.V., Ad Hoc Networks 3 (2005) pp: 257–279, 2005.

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

[10] Chai Keong Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002

[11] P. Gupta and P.R. Kumar. Capacity of wireless networks. IEEE Transactions on Information Theory, Volume 46, Issue 2, March 2000, doi:10.1109/18.825799

[12] Jump up^ Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2000

[13] Prasant Mohapatra, Srikanth V. Krishnamurthy, "Ad Hoc Networks Technologies and Protocols"

[14] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". *O'Reilly Wireless Dev Center*. Retrieved 2009-01-20

[15] Yi Qian, and Nader Moayeri,"Design Secure And Application-Oriented Vanet"

[16] P. Papadimitratos, V. Gligor, J-P. Hubaux, "Securing Vehicular Communications – Assumptions, Requirements, and Principles", Proceedings of the Workshop on Embeded Security on Cars (ESCAR) 2006, November 2006.

[17] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, October 2006.

[18] Tim Leinmuller, Elmar Schoch, and Frank Kargl, "Position Verfication Approaches for Vehicular Ah Hoc Networks", IEEE Wireless Communications, October 2006.

[19] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Priviate Vehicular Communications", Proceedings of the 7th International Conference on ITS Telecommunications, June 2007.

[20] Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, Vol.15, No.1, pp.39-68, 2007.

[21] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks", Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services, 2007.