The University of Nottingham

UNITED KINGDOM · CHINA · MALAYSIA

Comparative Study of Ad-Hoc Network Routing Protocols in Landslide Scenarios Using ONE

Aditya Purswani
Student ID: *20596344*
E-mail: *psxap13@nottingham.ac.uk*
MSc. In Computer Science

Coursework of Advanced Computer Networks (COMP4032)
Submission Date - 14 December 2023

under
Prof. and Dr. Dipl.Ing. Milena Radenkovic

School of Computer Science
University of Nottingham

Abstract:

Our aim in this paper is to simulate a scenario using ad-hoc networks, and opportunistic networks and to compare two benchmark algorithms aiding these networks using different metrics/ criterion based on the scenario. Opportunistic Networks (OppNETs) are special kinds of computer networks built over the paradigm of Ad-Hoc Networks (MANETs and VANETs), Unlike usual networking techniques where end-to-end connections are required to transfer the data. Opportunistic networks lack a path from source to destination and use transient connections.

In this paper, we will discuss and describe OppNETs and Information Centric Network Models in detail with various Delay / Disrupted Routing Protocols and how they can be implemented in a real-life scenario. We are using The Opportunistic Network Environment (ONE) simulator for the simulation setup. While discussing the scenario, we are taking two routing protocols into account for this experiment i.e. Epidemic Routing Protocol and Spray and Wait Routing Protocol. We will discuss and evaluate their performances under various circumstances. Our Scenario specifies the emergencies that might happen when a Natural Calamity especially landslides occurs and when the victims require fast and immediate supervision. We evaluated the performance and learned that Spray and Wait is a better Protocol than Epidemic and also discussed the challenges faced by these protocols. This paper will also discuss the pros and cons of DTNs in different scenarios.

General Terms: Performance Evaluations, Simulations, Emergency Scenarios

Keywords: Opportunistic Networks (OppNETs), Information Centric Networks (ICNs), Delay Tolerant Networks (DTNs), Ad-Hoc Networks, Opportunistic Network environments (ONE)

Introduction:

There are multiple cases where floods and landslides have affected a lot of lives. According to the Nature Journal, several thousands of people die due to landslides every year mostly due to lack of help. Many victims have died because they were not able to get proper help in time and were stuck in debris for a long amount of time. In this paper, we will try and discuss a way to deliver emergency messages to rescue centers and hospitals as soon as possible with the use of Opportunistic and Delay Tolerant Networks so that help can reach the victims as soon as possible.

Opportunistic networks have gained attention and popularity in recent years and are becoming more and more well-known in the community of researchers all over the world. The most important fundamental of opportunistic networks is that there is no need for an underlying infrastructure (topology) and that it makes use of connections as and when they are available. In traditional networks, communication depends on the assumption that there is a steady connection or a path between the sender and receiver (topology is static). On the other hand, opportunistic networks and ad-hoc networks are different and do not need any predefined infrastructure. Communication occurs with the unpredictable nature of connections, which allows nodes to communicate as and when they come in each other's range (proximity).

Here in this paper, we illustrate the use and importance of Opportunistic Networks (OppNETs) and also describe the working nature of nodes specified in these kinds of networks. Unlike conventional networks where there is a centralized server through which communication occurs, OppNETs uses peer-to-peer architecture where every node can behave as a client as well as a server based on the scenario's needs. This work provides a brief outline of ONE (Opportunistic Network Simulator) which is a Java-based GUI that is used while simulating the scenario by using prebuilt DTN routing protocols. It focuses on the evaluation of the performances of two benchmark protocols i.e. Epidemic and SnW (Spray and Wait) protocols by taking multiple criteria/metrics into account. After the evaluation of performance metrics, the paper will describe each and every metric with the use of graphs. In the final section of the paper, we discuss the pros and cons, advantages and disadvantages of using opportunistic networks / ad-hoc networks and DTNs, and also look at some scenarios where these kinds of networks might be useful.

1 Opportunistic Networks (OppNETs):

The moment opportunistic networks were introduced, truly revolutionizing the whole idea and understanding of networking. It changed the entire notion of conventional computer networks. As discussed many times in this paper, orthodox networks need the nodes to be, positioned in such a way that they form an end-to-end path for communication. Contrarily, in opportunistic networks, the message is passed without any established path between source and destination due to continuous change in topology because of node mobility.

1.1 Definition

The communications in an opportunistic network happen through wireless connections. All the nodes at any given point in time can be wirelessly connected with each other. The nodes in an opportunistic network may be either static or mobile or a mixture of both static and mobile nodes (in most scenarios it's hybrid). The connections between two nodes in a network for communication mainly depend on the node bandwidth (for eg. if it's a Bluetooth device then the connection/communication range will be less or we can define a larger bandwidth in ONE simulator). It allows the inter-communication of nodes if a fixed path does not exist between the sender and the receiver. Also, it is difficult to maintain a fixed path as the nodes are mobile and the topology keeps changing.

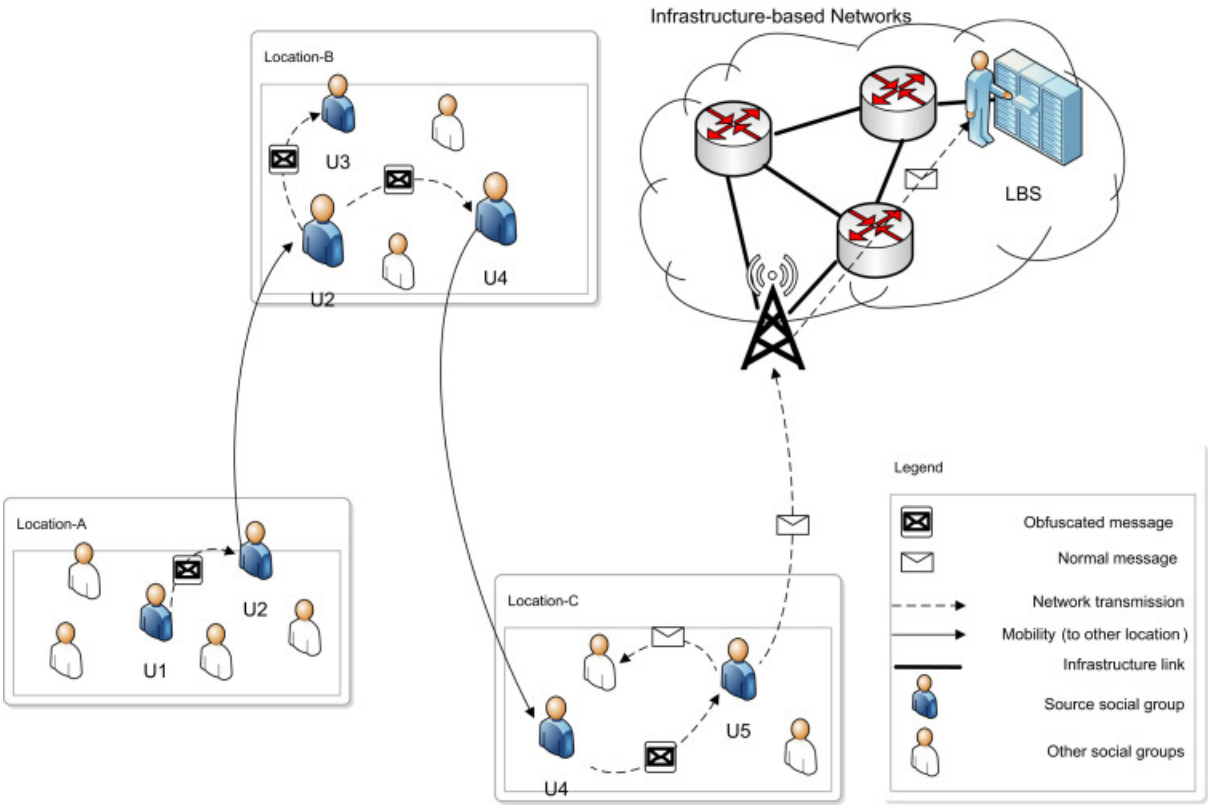

Fig 1 - Location-based security in OPPNeTs

How do nodes detect other network nodes?
If two nodes are in the communication range they will be able to detect each other and eventually will be able to transfer data to and from each other.

These kinds of networks can be complicated to understand because of their complex topologies, these topologies can be designed and understood with the help of temporal knowledge graphs (the edges can be created and destroyed at any time in a temporal graph). OppNETs are mostly used when there is no static connection/communication and no underline infrastructure for communication.

1.2 What are Mobile Nodes?

Mobile nodes in opportunistic networks can be any devices that can be wirelessly connected to any other device, and can be carried around in public for example: mobile devices (cell phones), laptops, tablets, LCDs, or any such handheld devices. Even any Augmented Reality device can be considered to be an Opportunistic Network node. As these devices contain wireless bands they can be connected over wireless networks. Also, cars nowadays are becoming smart so they can be considered nodes in these networks as they can possibly store much more data than a mobile device. So in conclusion, any device that has a wireless bandwidth and is able to form connections wirelessly can be considered as mobile Nodes. (these can be static or mobile/moving).

2 Information Centric Networks (ICNs)

Information-centric networking, unlike the normal host-to-host network paradigm where the focus is on end-to-end connectivity of hosts and the location of stored data, here the focus is on the information we need to identify. It does not matter in these kinds of networks where the information is located as long as we can retrieve the required information. For example [3] - if 5 people in the same proximity want to download the same data, it would unnecessarily use 5 times the internet. What we can do is one of them can download the data and share it in a group of 5 people. This way all of them get the message regardless of everyone's speed and fewer resources are used.

2.1 Definition

Before trying to discuss ICNs let us first see some drawbacks of the existing network paradigm i.e. that there is no representation of information (multiple copies of the same chink of data may be occupying space over the internet. Denial of Service might be one of the common problems that we might get to see because of this. [4] Nowadays we see that most of the traffic requests over the internet are related to access to content from companies like YouTube, Netflix, etc. The end users are interested in the data or information rather than where it’s coming from or how it's reaching them [5]. These high demands of large volume data such as videos were the motivation of paradigms like Information-centric networks

where architecture is based on named data objects rather than hosts being named [6]. This distinctively named data is used as a core principle in Information-Centric Networks.

2.2 ICN Communication Model

In Information-Centric Networks, the underlying network infrastructure constantly keeps caching the content/data available on the network and keeps distributing them to all the nodes in ICN. The main function of nodes in this network paradigm is to distribute the cached content and provide the requested content to the end user as and when required. When an end-user requests for some data in the ICN network, any node that has heard the request and has valid data for that request can respond to that request. We also face space and time decoupling here in these kind of networks [6]. Space Decoupling suggests that there is no need for the sender and receiver to know each other, the only thing or nodes they need to know are their partner nodes (nodes adjacent or near them). The caching mechanism here stores the recently and frequently made requests and stores them in cache memory so that they can be processed faster and response time can be as low as possible. This improves the quality of service (QoS) of the network. Also, these kind of networks take care of the security of data. The data is signed and sent so that it can be validated. As we can see in Fig 1 for normal traditional internet the data is picked directly from the location (content providers) while in ICN the data is picked from the nearest node that contains valid and complete data.

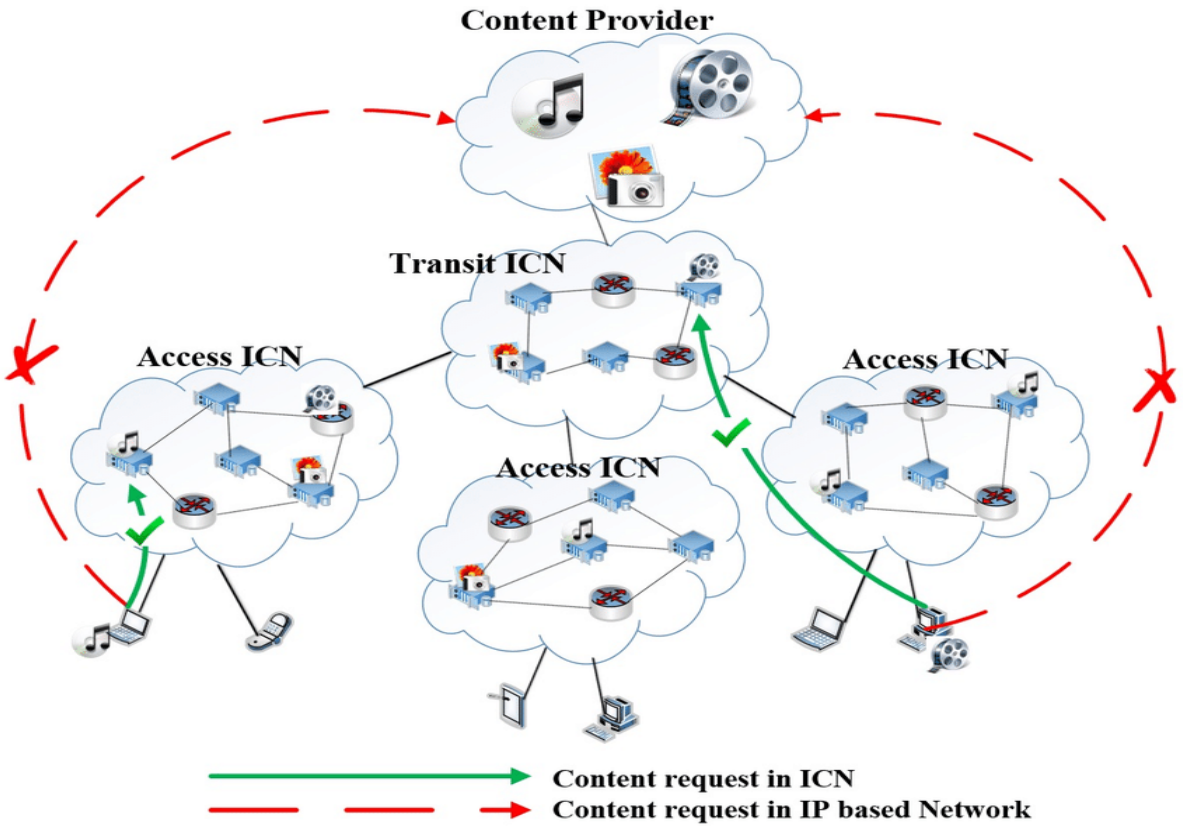

Fig 2 - ICN Communication Model

Content-centric networks are one of the most used types in ICNs. CCNs have a specific structure defined by which the data is represented and distributed across the networks.CCN naming is mostly hierarchical in nature. Caching of data is one of the main problems faced by ICNs. Many approaches have been tried and tested until now. There have been approaches such as collaborative caching [7] and forwarding. In [8] Zhang et al proposed a method for caching that is based on the popularity of data (the more number of times a data is requested the more popular it becomes). The networks smartly understand and separate the most popular content based on the requests made and store it in the cache for faster response times.

One of the main aspects of ICN is the naming of data. According to [9] the naming schemes can be hierarchical, random alphanumeric numbers, attributes that define the content, or hybrid data. The most used naming convention is hierarchical because this can be understood by almost anyone. Next, we have to describe the data, as if what is the content about. We need to provide suitable tags for the content so that our content is highly preferable in the network. For example - If the content is about landslides we can provide tags such as landslides, natural calamity, disaster, etc so that the content is relatable to the request made by the end user. So basically ICN is a far more efficient and resource-friendly approach rather than using TCP-IP approaches. The advantages of ICNs are that they are cost-effective in distribution, provide in-network caching, support multicast (data is distributed over multiple partner nodes), and its more secure and have improved privacy.

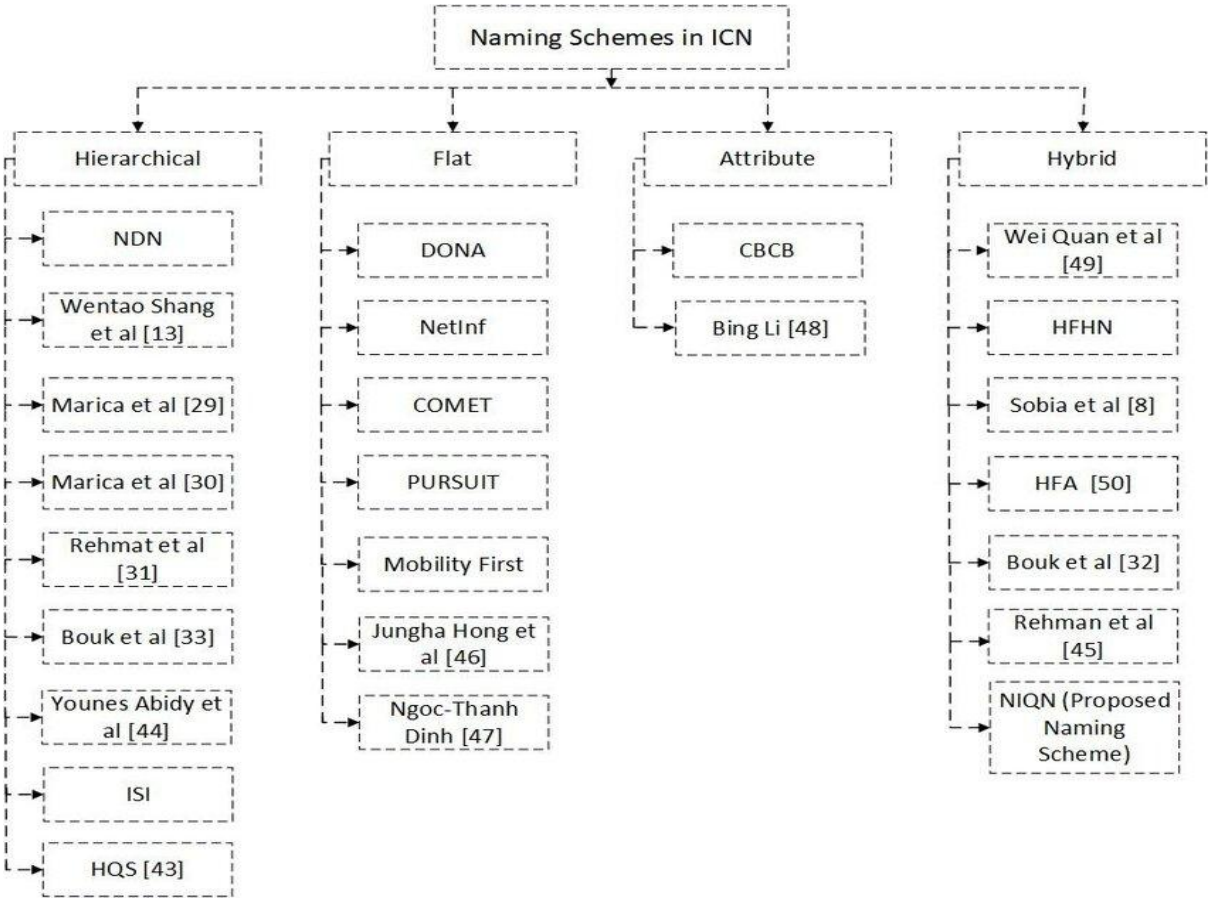

Fig 3 - Naming Schemes in ICN [9]

3 MANETs and VANETs

Ad-hoc as the name suggests something that is not planned happens, similarly in Ad-hoc networks, there is no predefined network infrastructure, no underlying path between the source and destination. They can be considered types of opportunistic networks. These kinds of networks allow all communications to happen on an intermittent basis (which means that the connection between two nodes is not permanent and can break at any moment). For Example - Two people want to share files between their laptops but there is no router or access points between the two nodes or laptops. Here Ad-hoc network connections can be very useful as they are direct peer-to-peer connections without the need of any external routing devices. These kinds of networks can be very helpful where there is a lack of network connectivity and important messages and files need to be sent.

There are various types of Ad-Hoc Networks presents -

a) Mobile Ad-Hoc Networks [10]
b) Vehicular Ad-Hoc Networks [11]
c) Wireless Ad-Hoc Networks [12]
d) UAV Ad-Hoc Networks [13]

Here we will briefly discuss about MANETs and VANETs.

3.1 What is MANET?

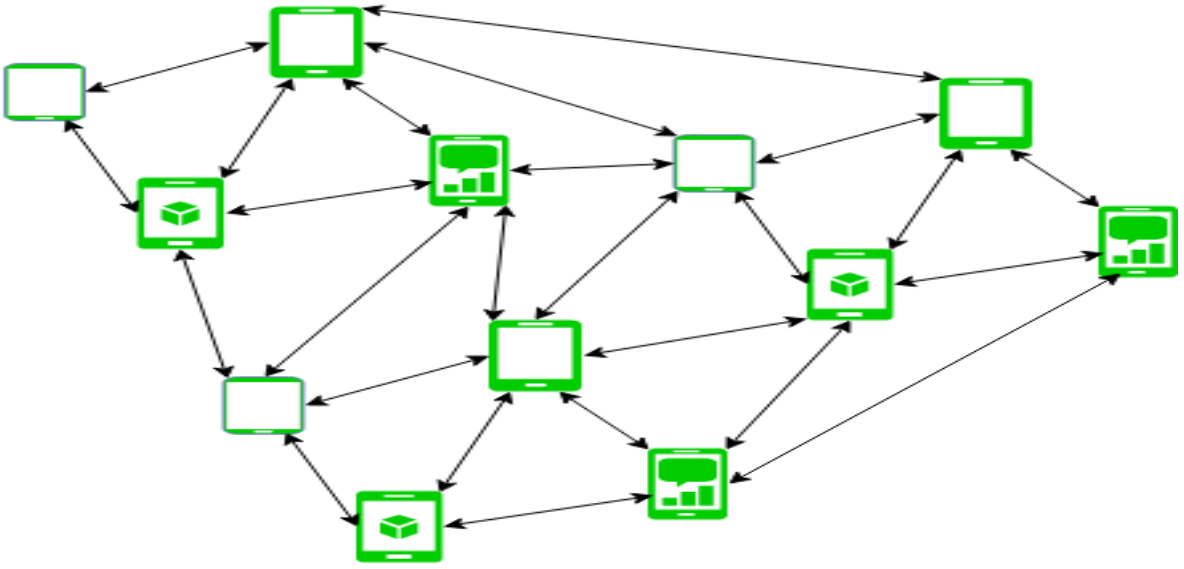

Fig 4 - Mobile Ad-Hoc Networks

MANETs also considered as Mobile Ad-hoc networks are a type of wireless ad-hoc networks that are self-constructing, self-organising, and infrastructure-less networks. These networks are known as self-constructing because do not have any external infrastructure, just there should be a type of connection between the mobile devices. They are self-organizing as

Mobile Ad-hoc networks do not have a static topology.[10] The topology keeps changing so the network has to organize itself to the changing topology and as we all discussed that for ad-hoc networks we do not need any underlying infrastructure. As we can see in Figure 14, different mobile nodes are connected to each other directly without the need for any centralized body or architecture. Every node is connected to each other via a wireless connection. The nodes in MANET move freely and randomly in the network infrastructure due to which the topologies are frequently changing. In this network, every node behaves as a router as they are responsible for data transfers to other nodes.

One of the main challenges that is faced by MANETs is the resources required to maintain the information required to route the data. Due to this successful routing of messages is one of the main concerns for these networks. As it's changing topology, there is two two-step process for routing i.e. secure multipath route discovery and data transmission which is mentioned in [14].

There are pros as well as drawbacks of using a MANET network. **Pros** are that is not centralized as traditional networking. There is no concept of separate hosts and routers, every node behaves as both nodes and routers. Mechtri et al. mentioned about the self-healing nature of MANET in [15] from which we can deduce that these networks require very minimal human intervention and these networks are very scalable in nature as we can increase and decrease the number of nodes as per the need of the individual or group. If we talk about the **drawbacks,** one of the major drawbacks is that MANETs are very resource heavy, and lack security features due to lack of authorization. These networks are more vulnerable to attacks and delays can be very huge as the topology keeps on changing and data keeps on moving in a loop.

3.2 What is VANET?

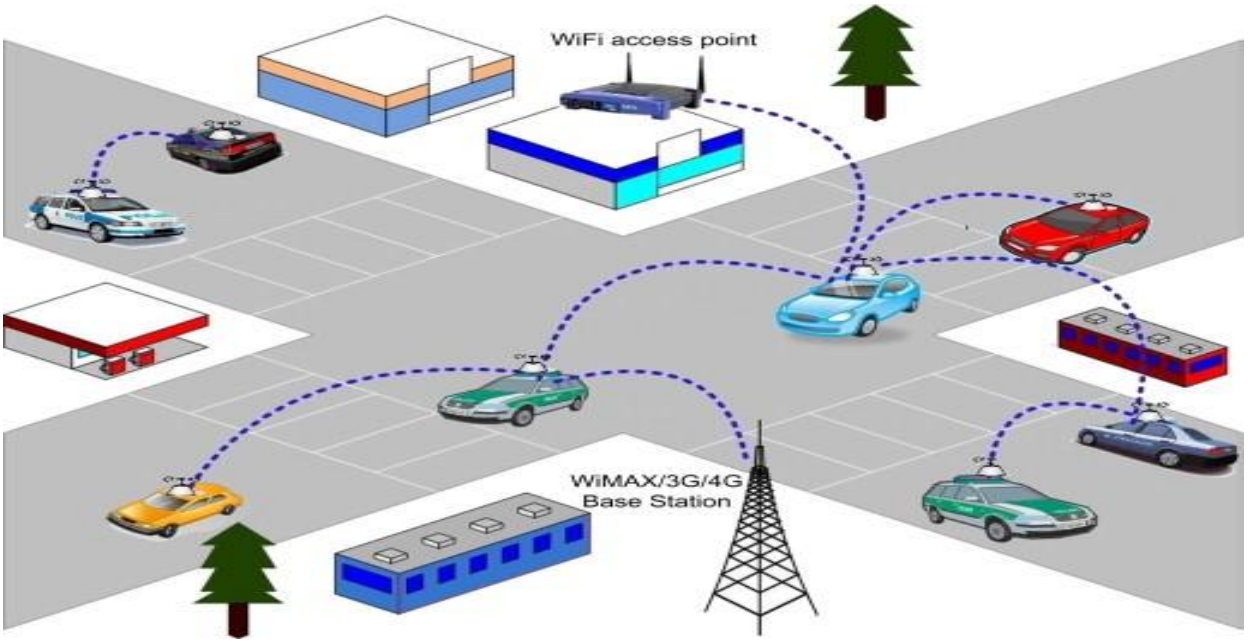

Fig 5 - Vehicular Ad-Hoc Networks

VANETs of Vehicular Ad-Hoc Networks are a unique type of MANETs that particularly use any kind of vehicle (2, 3, and 4 wheelers). As shown in Figure 5, there are two types of communications that can happen in VANETs, i.e. communications with other vehicles (a vehicle-to-vehicle V2V) connection. The second type of connection is a vehicle to a standalone body/infrastructure alongside the road (V2I) connection [16].

VANETs came into existence to increase road safety. A CartoCar consortium was developed as a standard. As we consider vehicles in these networks we have to talk about node mobility and organization of nodes. Cars move at high speeds which means that they have a high node mobility as compared to MANETs. High Mobility does not mean that nodes are free to move anywhere in the environment, they must have a limited trajectory and a limited degree of freedom. The organization of nodes is similar to MANETs as the nodes are self-organizing. Intervehicular communication IVC, discussed in [16] is a very old topic for research but it is still very popular in the research community. Network layer techniques for IVC communication are discussed in [17] and ad-hoc routing protocols including location-based, hierarchical, and geographical multicast routing, etc. are discussed in [18] and [19].

Although VANETs are similar to MANETs, there are some major differences that separate these two from each other. VANETs have 10 times more the bandwidth than MANETs, have higher scalability, and topology changes are very frequent due to high mobility. These are multi-hop networks and use a hop-by-hop technique to transfer the data to the destination. VANETs are divided into three categories - a) Pure Cellular, b) Pure Ad-Hoc, and c) Hybrid Networks.

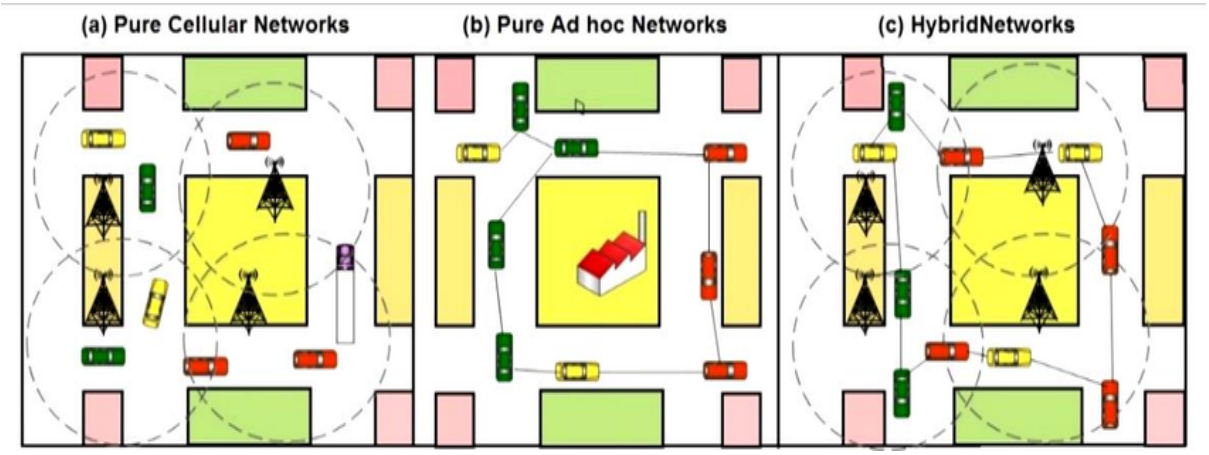

Fig 6 - Categories of VANETs - a) Pure Cellular, b) Pure Ad-Hoc, and c) Hybrid Networks.

In **Pure Cellular** networks, communication happens through fixed infrastructures or gateways on the side of the roads and not within the cars. **Pure Ad-Hoc** Networks are purely connections between mobile nodes and not with towers. **Hybrid** Infrastructure is the most used VANET of all as it combines the advantages of both. In our scenarios, we will be using a mixture of MANETs and VANETs because our scenario contains pedestrians and cars.

4 Delay/Disconnected Tolerant Networks aka DTNs

In this section, we are going to discuss Delay/Disruption Tolerant Networks and why they are important for routing in Ad-hoc networks. We will also see a few routing algorithms made on the delay tolerance approach.

4.1 What are DTNs?

Delay Tolerant Network provides a solution to one of the major disadvantages of MANETs and VANETs. Due to high mobility and transmission range being low, there can be unstable and unreliable connections [20]. DTN routing is used mostly in environments where networks are disconnected and disrupted very easily and the relay of messages is impossible. Without the use of DTN algorithms, it might be possible for nodes to drop the message before passing it to other nodes. Due to this, we suffer huge message delays and drops in MANETs. From this discussion, we can understand that DTNs are utmost useful in the networks when there is no specific path to the destination and connections established between the nodes are transient.

4.2 DTN Routing Protocols

DTN or Delay Tolerant Networks uses the store-carry-forward paradigm. In this paradigm, as shown in Figure 7a, each node stores some data/information in its buffer and carries the data along with it until they do not meet any other nodes. Once the node meets another node, they create a session where they transfer data that is not seen by them yet. Using this mechanism/paradigm, various routing algorithms have been made that emphasize message delivery and resource consumption. The communication in different regions as shown in

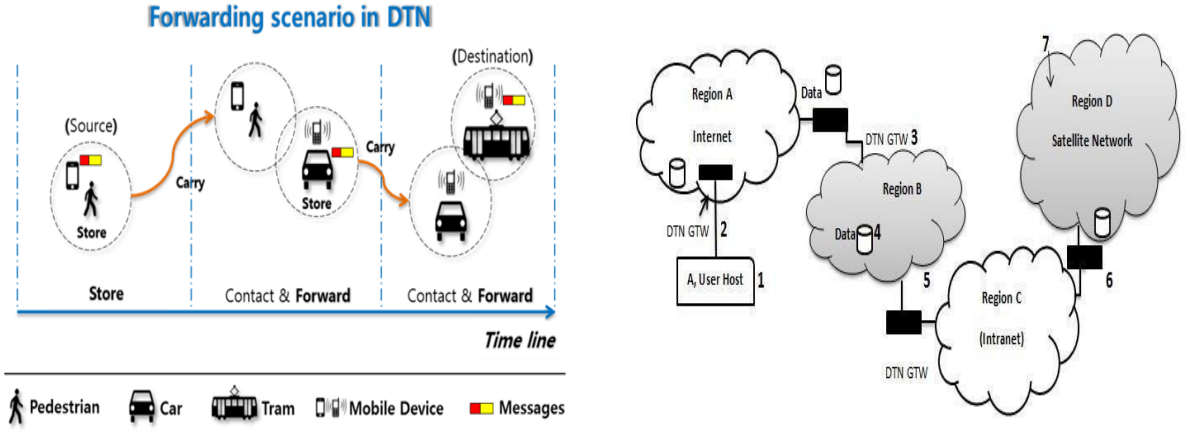

Fig 7 - a)Store-Carry-Forward b)Architecture of DTN

Figure 7b above is happening due to the DTN gateway at local borders of the region explained in [21]. DTN routing is divided into two types - a) Forwarding Based, b) Replication Based

Forwarding-based routing protocols are one of the most simplest protocols to understand and implement. As the word displays a single copy of the message is forwarded in the network until it reaches the destination. Message can be handled by only one node at any instance of time. Although it takes fewer resources and space but message delays are very huge.

Replication-based routing protocols are the most known and used algorithms in DTN, where a single message is propagated through the entire network via replica copies of messages. The nodes transfer messages as copies of original messages and still contain the original message with them. So, basically, at a time there might exist multiple copies of the same message in the network. The main disadvantage is that these protocols consume a lot of resources.

However, in this study, we are going to use Epidemic and Spray and Wait protocols and study about that. (detailed explanation in Section 6)

Here we will discuss some of the Replication-based protocols -

4.2.1 Epidemic Routing Protocol

Epidemic routing [22] is one of the initial protocols that was introduced using the replication technique. This protocol takes advantage of flooding, as the name suggests it floods the network with message copies. When in range two nodes share the copies with each other that they have not seen and move on until either their message hash is full or they have reached the destination. The main disadvantage of this protocol is that it uses a lot of resources because multiple copies of the same network are roaming in the network.

4.2.2 Spray and Wait Routing Protocol

Spray and Wait [23] is considered an advanced version of epidemic protocol, as instead of replication messages blindly it sets an upper limit to how many times a message can be replicated. We can utilize the resources efficiently as the limit is set according to the resources available while still having a high message delivery probability. It has two phases a) spray phase and b) wait phase

In the **Spray Phase** initially the source node creates a message, and an upper limit **L** is associated with that message determining the number of message copies. So spray phase propagates the messages to multiple nodes.

While in the **Wait Phase,** once the copies value has reached 1, only direct transmission to the destination can occur. In other words, the node will wait until it meets the destination to transfer the message as it cannot disseminate the message any further.

4.2.3 MaxProp Routing Protocol

This routing protocol like Epidemic follows the principle of flooding and propagates the messages throughout the network. The main difference in both networks is that in MaxProp [24] an ordered queue is maintained as a message buffer to know which messages we have to drop. This queue is ordered in such a way that the messages that have the most probability of reaching the destination are given priority in forwarding. Now the main question is how this probability is decided. In each node, MaxProp maintains a history of collisions/encounters between two nodes to maintain a vector of the likelihood of messages reaching the destination. The vector is exchanged at the time of encounter of two nodes.

4.2.4 Prophet Routing Protocol

Probabilistic Routing Protocol using History of Encounters and Transitivity otherwise known as PRoPHET [25] also maintains a vector that maintains a track of nodes that are already encountered. While replication PRoPHET calculates a subset of nodes to which the messages can be replicated. Then these nodes are ranked in order of probabilities in the vector and messages are copied to the highest-ranked nodes. The calculation of probabilities is known as the training phase.

5 The ONE Simulator

In this section, we will have a look at the simulation environment used to simulate the scenario depicted. We will briefly discuss different ways to access the simulator. How it works? How nodes are moved? We can run our simulation through CLI as well as GUI interfaces respectively. We will also discuss the commands by which we can run the simulator.

5.1 Introduction to ONE Simulator

ONE [26] is the abbreviation of Opportunistic Network Environment Simulator in which we can simulate real-world scenarios using different DTN algorithms and determine which protocol gives us the best delivery using the least resources in any given scenario. ONE simulator environment provides us with features such as the formation of node groups, node communication with each other, node movement, report generation, routing protocols, and event handling or message handling. As we can see in Figure 8, the architecture of ONE simulator depicts the main components i.e. movement models, event generators, simulation engine, routing, and visualization and results.

We can access the ONE simulator environment using a CLI or GUI interface. We will now how to access the GUI interface using CLI.

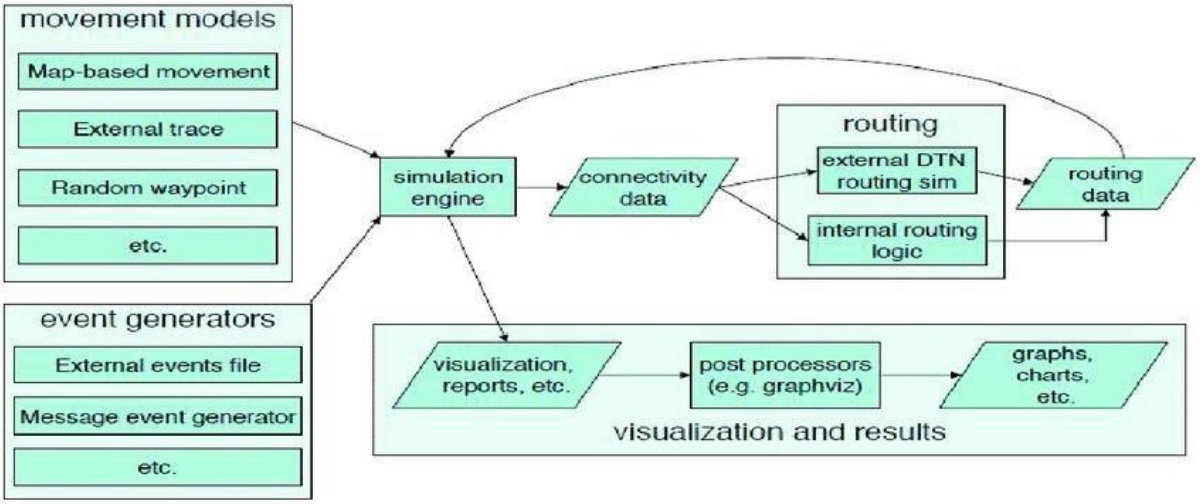

Fig 8 - The architecture of ONE simulator

For Windows Users -

>> compile.bat <config-file name.txt>

>> one.bat <config-file name.txt>

For Mac Users

>> sh compile.sh <config-file name.txt>

>> sh one.sh <config-file name.txt>

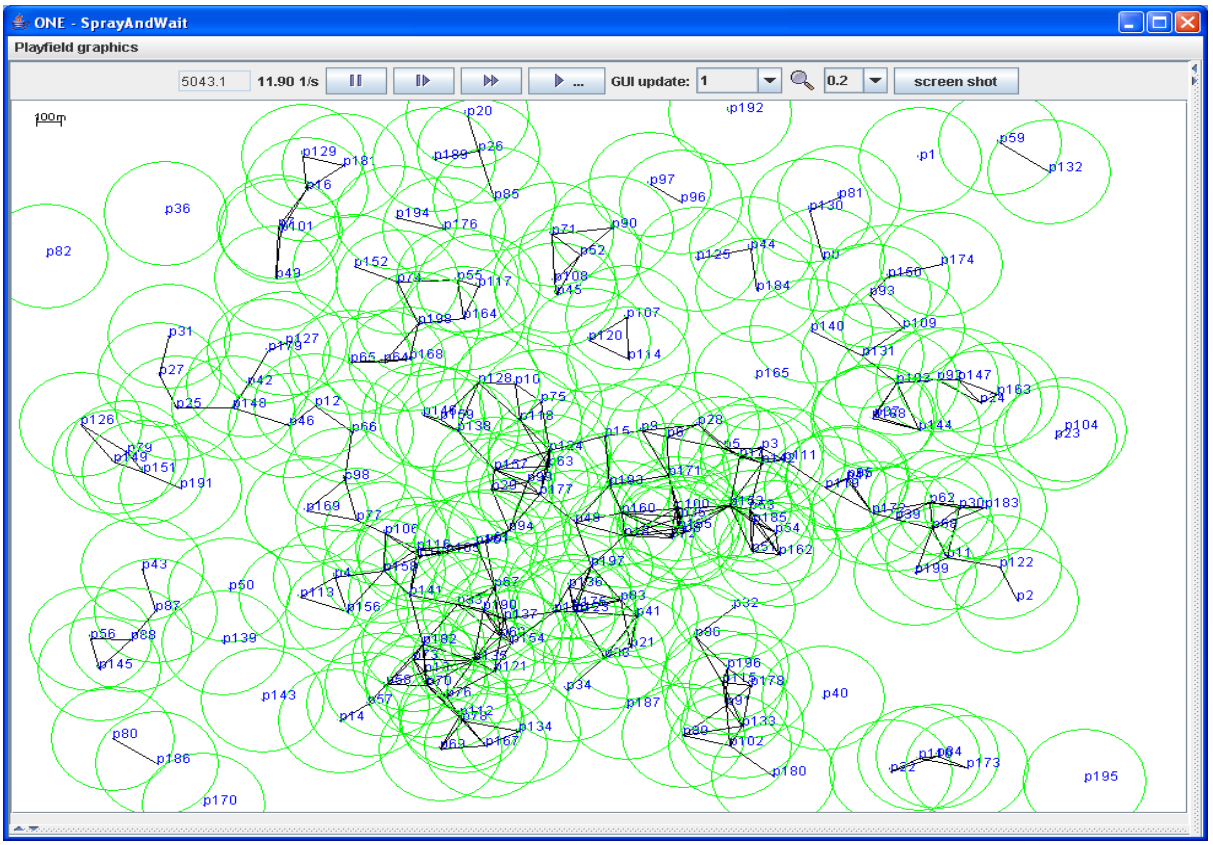

Fig 9 - ONE Simulator Environment

One.sh and One.bat commands are used to access the GUI interface shown above in Figure 9. The simulations in the GUI interface can be viewed in real-time and as soon as the simulation finishes the data and the result reports are generated from which we can deduce the outcomes. Another thing is that we can view the path on which a node moves by clicking on the node number at the side scrollbar.

5.1.1 Nodes Movement

For Node Mobility, some movement models are implemented in ONE simulator that helps us predict or generate the movement of nodes. We can either use movement models that are pre-defined in the simulator or load our own external traces of any other map and use them as movement models to run the simulator. Some of the most popular movement models that are used in ONE are Random Walk and Waypoint. The models were simple to implement and understand but had a lot of limitations specifically because the node movement path was randomly decided which was difficult to explain in every scenario. These were random traces that changed in every run.

ONE provides us with some more movement models that are more intuitive in terms of real-world scenarios. These node movement models have predefined paths on which the nodes move. Some of the models are Map Based Movement (MBM), Shortest Path Map Based Model (SPMBM), and Routed Map Based Model (RMBM). For pedestrians, cars, trams, etc ONE uses the Helsinki map data to determine the sidewalks, roads, etc using .wkt files. For static nodes, we can use Stationery Movement.

5.1.2 Routing Protocols Implemented

As we discussed in the previous section there can be various routing protocols that can be implemented while working in an Ad-Hoc environment. ONE simulator is stocked with some of these protocols that we can use while working with our scenarios. ONE simulator has a basic framework for defining the algorithms by using DTN routing protocols. Some of the most popular protocols that ONE Simulator provides are - Direct Delivery (DD), First Contact (FC), Epidemic, Spray and Wait (SnW), PRoPHET, and MaxProp. [26]. Although ONE simulator is a 2D simulator and cannot be used to simulate drones and satellites, still it is very powerful and useful to study most of the real-world scenarios. These routing protocols perform the same steps in node communications and deal with the messages in a similar way until it's delivered to the destination because the underlying architecture is the same.

5.1.3 Types of Reports

While conducting any study or experiment, the result generation and the detailed comparison and understanding of the results are very important. To compare the performance of different protocols for the scenario ONE simulator provides us with different types of reports that log multiple values while we run the simulation. A few of them are - ConnectivityONEReport

which logs the connectivity formation between nodes, DeliveredMessageReport which tells us about the number of messages delivered, MessageStatsReport that gives us the statistics about the messages delivery, creation, latency, ratios, messages dropped, etc. according to the protocol used. There are many types of reports that we can use for a better understanding of the study or scenario.

5.1.4 How Messages Are Handled?

In ONE Simulator messages are handled using event generators, these event generators generate events in which the message creation interval is defined, sources that generate the messages are defined, and destinations that are meant to receive these messages are defined.

Events.hosts is used to define the source nodes whereas Events.tohosts is used to define the destination nodes. Once we define all these then these messages will be created by source and transferred according to the protocol defined in the config file. These messages are relayed to the next node once two nodes are in contact. Once the message is received by the destination, it is removed from the hash table of the nodes containing that message, or if the congestion is more it might be possible that the message is dropped before reaching the destination.

6 Landslide / Natural Calamities Emergency Scenarios

In this section we are going to discuss the scenario we are looking at in this study in detail and why talking about such scenarios is necessary. We will then discuss the config files and Environment Setup and the protocols used in this study in detail.

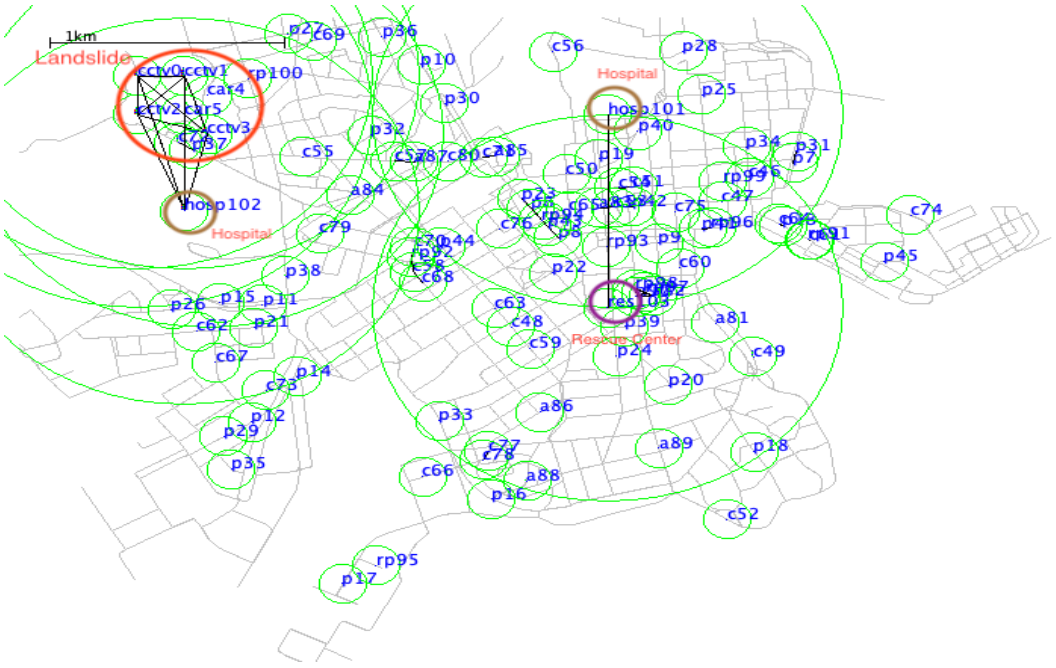

Fig 10 - Scenario Playfield

6.1 Understanding the Scenario

As we all know natural calamities such as landslides, floods, and tycoons can cause havoc in human settlement areas and can be devastating for human lives. One such scenario is landslides which is the main reason why we are conducting this study to develop a network in landslide-prone areas such that rescue teams can get to the location as fast as possible and save as many lives as possible. To Understand the scenario we need to first understand what are Landslides and what effects can they have on human life.

Landslide is a phenomenon that is defined by the sudden movement of tectonic plates and due to that the downward movement of rocks, sediment, and debris. These can also be caused by to lack of vegetation in the area. Landslides can triggered due to various manmade and natural causes. Natural causes include earthquakes, floods, volcanic eruptions, etc. On the other hand, the human activities triggering landslides are mining, deforestation, construction of land near water bodies, etc. The consequences of Landslides can be severe too. These landslides are dangerous as many people might lose their lives and homes etc. It can also lead to the destruction of infrastructure that is the only way for some people's daily commute like roads, bridges etc.

Our scenario looks into a landslide that occurred in a sloppy area that is landslide-prone. Due to landslides, some cars come under the debris of landslides. And there is no way for the people can communicate from under the debris for rescue. Every year many people lose their lives in the same way. Especially in India in the Uttrakhand Region, every year in the rainy season due to heavy floods many people die or have to move to a different place as their homes are drowned in floods

Fig - 11 Landslide in Uttrakhand

To overcome this Ad-Hoc Networks can be used so that help can reach the victims as soon as possible. In this scenario, with the help of CCTVs, we will send the live footage of the

landslide using different nodes such as pedestrians, cars, and ambulances, so that this footage can reach the rescue centers and hospitals so that they can be prepared for the number of people stuck or injured from this accident. The main aim of studying this scenario is to establish a strong network that can prove to be helpful in disaster-prone areas and with the help of these networks, the lives of people can be saved.

6.2 Simulation Set-up / Understanding Config Files

To run any simulation file it is necessary to understand the config files, what they contain, and how to access and run them. This study aims to compare epidemic and spray and wait routing protocols in an emergency scenario such as landslides, compare their performance across various metrics, and hence decide which one is better than the other. To do this in the simulation we have taken a total of 13 groups. The first 5 groups are to define CCTV cameras as they are static and need a separate group for each of them. Other groups are pedestrians divided into local people, rescue personnel, and doctors. Next are cars divided into local transport, ambulances, and rescue vehicles. Finally a rescue center and hospitals.

Criterion	**Values**
Simulation Name	Landslide_epidemic and Landslide_SnW
Scenario Run Time	10800 (3hrs)
Movement	Shortest Map Based Movement and Stationery Movement
Number of Node Groups	13
Number of Nodes	104 (varies while comparing)
Time to live	300 minutes
Map Used	Helsinki
Interfaces Used	Bluetooth and High-Speed
Node Buffer Size	120 MB

Table 1 - Criterion and values for the scenario

In this study, we are using both Bluetooth and high-speed interfaces where Bluetooth is depicted by mobile phones with pedestrians and cars, and the high-speed interface is depicted by walkie-talkies with rescue workers, and rescue centers, and hospitals. We are simulating this in the Helsinki environment but assuming that the environment is a landslide-prone area such as Uttrakhand or a recent landslide that occurred in Alaska. In the configuration file, we also looked at the speeds of cars and different metrics according to which we will compare the two protocols in the next Section.

6.3 Benchmark Routing Protocols Used

In this section, we are going to discuss the benchmark protocols used in the study for comparison in the landslide debris scenario.

6.3.1 Epidemic Routing Protocol

The Epidemic protocol [22] is one of the most basic and easily understood replication-based protocols. Epidemic is considered the first routing protocol invented for a divided network containing transient connections. Vahdat and Becker introduced a flooding-based approach keeping only one thing in mind which was to solve the problem of message delivery without considering the resources used. The flooding approach simply means to flood the network with message copies such that every node or at least most of the nodes have the copies so that message delivery is sure. Epidemic as we now replicate a message into multiple copies and every node that has a copy is responsible for that message.

The main goal of this protocol was to achieve high message delivery in the networks that do not have a connected space all the time and connections are transient due to the dynamic mobility of nodes. The message copies are transferred when two nodes come in range of each other. When two nodes are in range they form a session in which they share each other's details along with summary vectors. These summary vectors contain all the information of all the messages that a node holds.

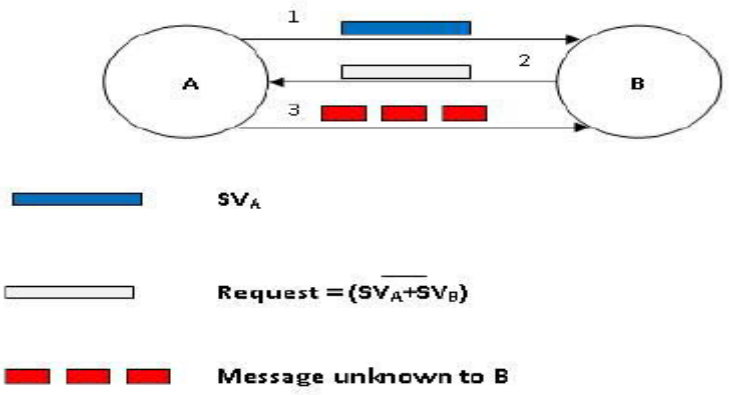

Fig 12 - Summary Vector Exchange

As shown in the figure above A shares its summary vector with B, then B reads the summary vector, searches for the messages that B does not have, and takes those messages as copies from the summary vector of A. This is done by a logical AND operation that B performs. B then requests A to transfer the messages from A's summary vector according to the logical operation. A then sends the messages that B had requested and that is depicted by the red dashed line.

In this session, the message is forwarded to the other node and this process keeps on repeating until the node has reached the destination or it has been dropped. Because at any given time there are hundreds of copies of a message in the network the resources used in this network are very huge at times not present in real-world scenarios. This is why even though it is the easiest to implement and understand the message latency and overhead ratios are very high in any scenario.

6.3.1 Spray and Wait Routing Protocol

The Spray and Wait protocol as discussed earlier in this study was proposed keeping the use of resources in mind. This protocol uses the resources efficiently without affecting the message delivery drastically. Spray and Wait Protocol contains two phases 1) Spray Phase & 2) Wait Phase. In the Spray Phase messages copies are transmitted to only a specified number of nodes from the root node. This protocol was introduced to resolve the problems faced by all the protocols that were introduced before such as minimizing the delay and overhead ratio, optimizing the use of resources, and maximizing the message delivery with the resources available.
The spray phase is continued until the number of message copies is reduced to 1. When the message copies are 1 then the protocol enters the wait phase and initiates the direct transmission protocol because the message can no longer be divided or copied.

The Spray Phase is described in 2 ways- 1) Vanilla and 2) Binary and the wait phase is common for both of these.

6.3.1.1 Vanilla

Vanilla Spray and Wait is the easier of the two to understand and implement. In this version suppose N is the number of copies that are to be sprayed over the network. During the Spray Phase in this version, a node that wants its messages to get delivered to the destination will forward one copy to N-1 unique nodes. As the transmission starts, for each transmission the node decreases N copies by 1 local copy.

This process is repeated for every message that is delivered to the destination. Once the number of copies reaches 1 the protocol enters the Wait Phase.

6.3.1.2 Binary

Binary Spray and Wait is more complex but uses the resources more efficiently. In this version suppose N is the number of copies that are to be sprayed over the network. During the Spray Phase in this version, a node that wants its messages to get delivered to the destination will forward N/2 copies to another node, leaving it with N/2 copies. Once the node is left with 1 copy it enters the Wait Phase.

The main advantage here is that the message copies are distributed very quickly and more nodes are responsible for distributing the message instead of the node that created the message.

6.3.1.3 Wait Phase

Now, we know when the Protocol enters the Wait phase, Once the waiting phase is in motion all the nodes with the message copies try to directly transmit the information to the destination. The nodes wait for themselves to come into contact with the destination and then transmit the message to the destination. The main problem is to find N here for the spray phase because it is computationally expensive.

7 Performance Evaluation / Result Comparison

In this section, we will consider multiple metrics and compare the performance of the protocols discussed in the previous section namely Epidemic and Spray and Wait.

7.1 Result Overview

Here, we will look at all the metrics we consider and how they affect the scenarios. The metrics include the total number of nodes, speed of nodes, buffer sizes, transmission ranges, positions of sources and destinations, and many more. The effect of changing these metrics on the performance is as follows:

Total Number of nodes - By increasing or decreasing the total number of nodes, the effect is directly on congestion in the network. If the nodes increase, congestion increases, and vice versa. And congestion directly affects the message delivery. The more congestion in a network, the less the message delivery success.

Speed of Nodes - If we increase or decrease the speed of movement of nodes, it directly affects the time two nodes are in connection with each other. Less speed means nodes will be connected for a longer period and vice versa.

Buffer Sizes - directly translates to the number of messages a node can hold at a time within its cache memory to transmit to other nodes. Buffer Sizes determine the message holding capacity of a node.

Transmission Range - determines the range of message transmission, the range in which nodes can connect to each other and start the process of message transfer. The more the transmission range, the more the transaction between nodes. But the main problem here is the use of resources. Bigger transmission ranges use more resources.

Position of Source and Destination - One of the main metrics as it determines how fast a message can be delivered or how slow a message is delivered. If sources and destinations are close to each other the messages will reach there very easily and quickly.

Now in the next section, we will see the performance evaluation of both protocols with the help of graphs on some of the metrics discussed above.

7.2 Comparison of Protocols on Various Criteria

Here we first discuss the message sizes considered, as the scenario contains CCTVs to send the recorded footage the message size will be larger as they will be images and videos. The message sizes that we consider here lie in the range of 2MB to 5MB as we will be sending clips of the accident or landslides to destinations. For nodes to retain messages our buffer sizes need to be high enough so that they can at least hold 5-10 messages at a time. Because in real-world scenarios the buffer should contain a minimum of 10-20 messages at a time without dropping a message. We also need to know that in this scenario we are using both Bluetooth and high-speed interfaces because hilly terrain does not have Wifi at all times.

Firstly, in this comparison, we will constantly increase the **buffer sizes of nodes** and see the effect of it when the scenario runs -

In the tables shown below, we have every value to properly compare and evaluate the two protocols while we fluctuate the buffer sizes. We take messages created, started, relayed, aborted, and many others into account. We will look into every value one by one and compare the two protocols.

	Epidemic 30MB	Epidemic 50MB	Epidemic 60MB
Messages Created	901	901	901
Messages Started	15004	19857	19857
Messages Relayed	13868	14839	14839
Messages Aborted	1133	5001	5001
Messages Dropped	14430	15363	15363
Messages Delivered	208	224	224
Overhead Ratio	65.6731	65.2455	65.2455
Delivery Probability	0.2309	0.2486	0.2486
Latency Average	26.8803	109.8348	109.8348
Hop Count Average	1.1923	1.5893	1.5893

Table 2 - The effect of changing the buffer sizes on the message delivery in Epidemic Protocol

	SnW 30MB	SnW 50MB	SnW 60MB
Messages Created	896	896	896
Messages Started	3880	3890	3892
Messages Relayed	3837	3846	3848
Messages Aborted	43	44	44
Messages Dropped	3889	3826	3814
Messages Delivered	362	367	369
Overhead Ratio	9.5994	9.4796	9.4282
Delivery Probability	0.4040	0.4096	0.4118
Latency Average	233.5508	273.8166	287.1897
Hop Count Average	1.1133	1.1253	1.1301

Table 3 - The effect of changing the buffer sizes on the message delivery in Spray and Wait Protocol

As we know, Epidemic protocol replicates the message to every node it encounters so the messages started in Epidemic are significantly Larger than Spray and Wait because in Spray and Wait we specify a value N which are the number of copies to be transmitted. This is the reason why dropped, aborted, and relayed messages are related in the same way in both the protocols.

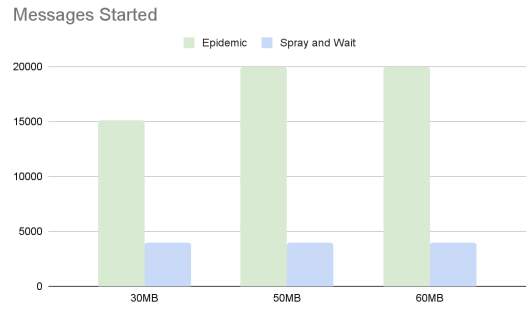

Chart 1 - Messages Started

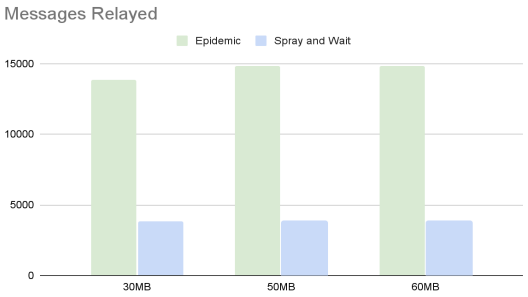

Chart 2 - Messages Relayed

Messages Relayed reflect the contacts and transfers of messages between the nodes. The messages Relayed in Spray and Wait are significantly lower than in Epidemic because Spray and Wait has an upper limit to replication which Epidemic does not have. Through the above two graphs, it can be seen that there is a clear correlation between messages started and messages relayed. As for Epidemic, the messages started are more so, it's obvious that the messages relayed will be more and vice versa for Spray and Wait.

Chart 3 below shows us the dropped messages, i.e. the messages that are dropped before getting delivered or failed to be delivered due to some or the other limitation. These limitations can be anything such as the buffer being full or congestion in the network. From the chart, we can figure out that SnW does a nice job as dropped messages are very less as compared to the epidemic.

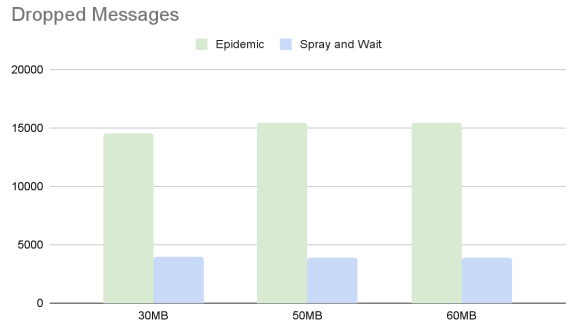

Chart 3 - Dropped Messages

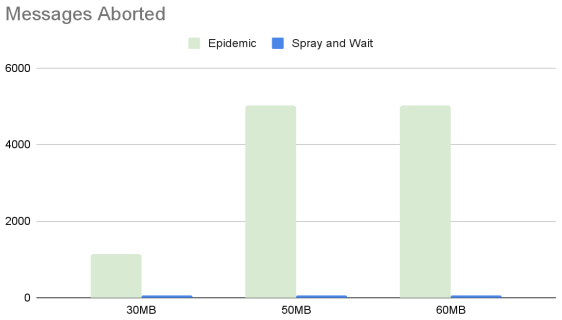

Chart 4 - Messages Aborted

As we can see in Charts 5 and 6 below when we increase the message delivered increases by some amount in both the Epidemic Protocol and Spray and Wait Protocol and the same we can see through the delivery probability. These show us how the two algorithms work for delivering the messages. Spray and Wait protocols are more appropriate in terms of message delivery than Epidemic protocol. The probability is low because the messages here are big as they contain videos and images.

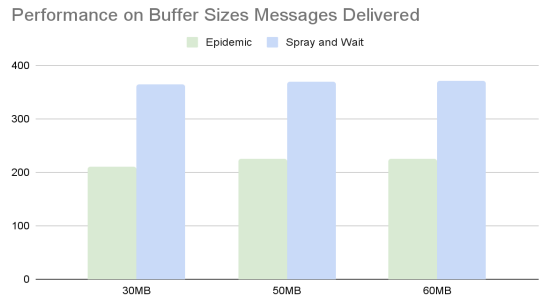

Chart 5 - Messages Delivered

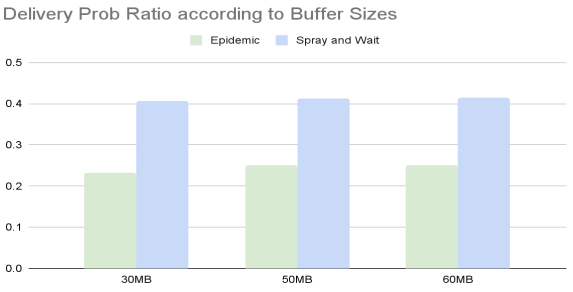

Chart 6 - Prob Ratio

Chart 7 below shows us the overhead ratio or the expense of transmitting the message from source to destination. Spray and Wait are significantly lower because in it we can control the number of copies that are being transmitted over the network while the Epidemic focuses on increasing the delivery probability by replication of messages without an upper limit. This basically depends on the amount of extra data we send with the message.

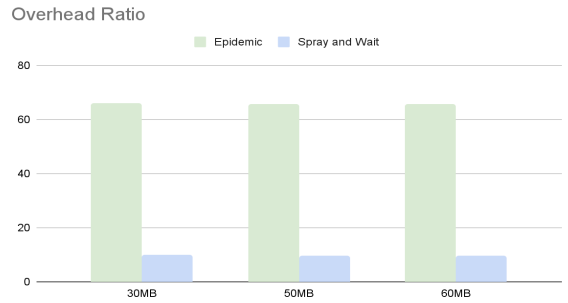

Chart 7 - Overhead Ratio

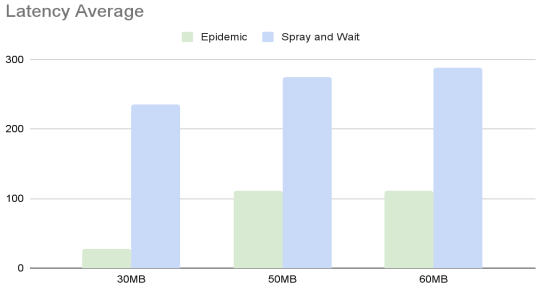

Chart 8 - Latency Average

Whereas, Chart 8 shows the latency average, which is the time it takes from the message creation at the source to the message delivery at the destination. Spray and Wait routing protocol tries to minimize the latency by copying the number of messages but the Latency in Epidemic is much lower as it floods the network with message copies so it is clear that Epidemic will be faster.

Now we will see the comparison based on the number of nodes **(network density)** -

Here while comparing we are considering low network density (59 nodes) and high network density (104 nodes), which we are going to compare the values of message delivery, dropped messages, latency average, and overhead ratio.

	Epidemic Less Density	**Epidemic More Density**	**SnW Less Density**	**SnW More Density**
Messages Started	14555	15004	3739	3880
Messages Relayed	14483	13868	3676	3837
Messages Dropped	15053	14430	4104	3889
Messages Aborted	70	1133	62	43
Messages Delivered	292	208	429	362
Delivery Prob	0.3241	0.2309	0.4761	0.4040
Overhead Ratio	48.5993	65.6731	7.5688	9.5994
Latency Avg	9.7442	26.8803	9.8012	233.5508
Hop Count Avg	1.2808	1.1923	1.3636	1.1133

Table 4 - Comparison of Values based on Density of Network

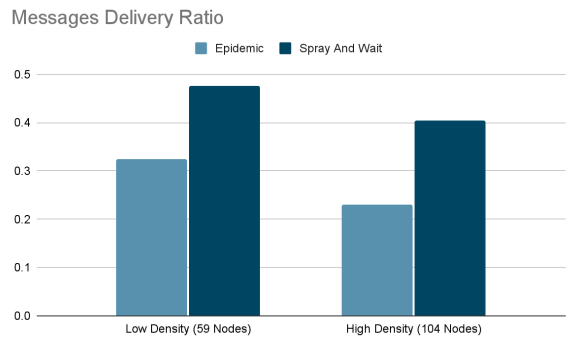

Chart 9 - Dropped Messages

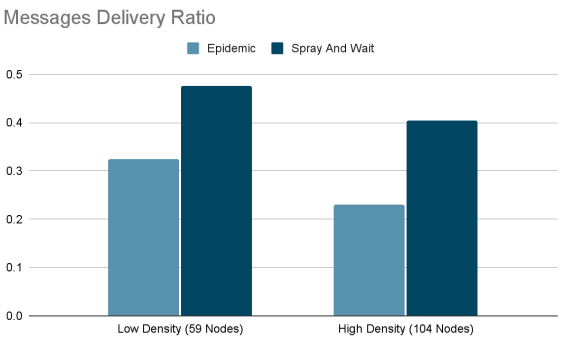

Chart 10 - Latency Average

As seen in Chart 9, The messages dropped are decreasing as the network density increases in both Spray and Wait and Epidemic. This may be possible because as the density increases, there are more nodes and thus more total buffer space available for the messages to be stored in. But here also the messages dropped in Epidemic are significantly higher than SnW because of the same reason that dropped messages are in correlation to the messages started. Epidemic creates more copies of messages hence the drop is significantly higher.

Chart 10 shows us the latency average and we can see that it does not matter if the density is less because the latency of both protocols is similar to each other. This can be because congestion is significantly less so nodes can reach the destination easily. When the density is higher Spray and Wait faces a higher latency average because it does not replicate many copies when compared to Epidemic

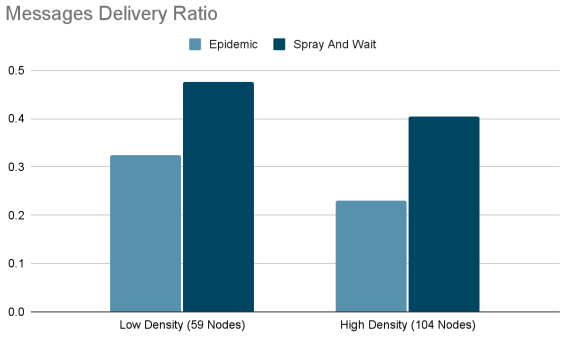

Chart 11 - Delivered Messages

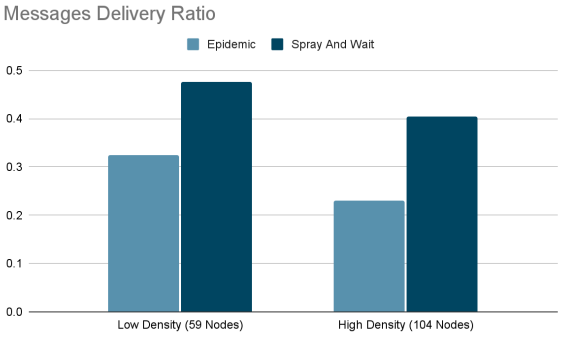

Chart 12 - Message Delivery Ratio

As shown in Charts 11 and 12, we can evaluate that when network density is less the message delivery is increasing for both protocols as the congestion in the network is less, hence more number of messages are reaching the destination. While, when density is high the delivery probability is high. Although Spray And Wait delivers more messages than Epidemic in both cases.

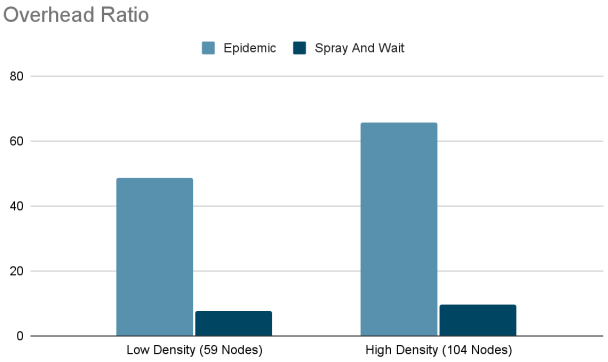

Chart 13 - Overhead Ratio

Chart 13 shows the increasing nature of the overhead ratio as the density increases, this is also because of the same reason as congestion increases the resources used by the network also increase hence the overhead ratio increases. While protocol-wise Spray and Wait are significantly lower because in it we can control the number of copies that are being transmitted over the network while the Epidemic focuses on increasing the delivery probability by replication of messages without an upper limit.

According to the analysis of metrics, we can clearly see that in this scenario Spray and Wait is a better protocol here as it delivers the messages more appropriately and consistently as compared to Epidemic Protocol

7 Pros and Cons - DTNs and Opportunistic Networks in Various Scenarios

In this section, we will discuss various scenarios including ours, and evaluate the pros and cons of Ad-Hoc and DTN networks in these scenarios.

In the scenario discussed in this paper, natural calamities such as landslides DTN, and ad hoc networks can be most useful as traditional network fails in such scenarios because the network connectivity in an area of destruction is very low. So networks such as Opportunistic networks can be most useful as they do not need an underlying infrastructure. The network can be developed by the resources and devices available. As in our case CCTV cameras, pedestrians, and cars. The major advantages of these networks are that they can be the difference between life and death as help can reach the needy in time. These networks are self-configured with minimal human intervention. So it makes these networks robust. Some problems that we can face are congestion, less security, authorization, and use of lots of resources.

Other scenarios in which there are applications of DTN and ad hoc networks are Military Operations. This is one scenario where we need a decentralized network because data is very sensitive and can affect an entire country. In this network, only the soldiers and the headquarters can have access to the network and no one else. Military operations are very sensitive and can lead to a World War so we can’t risk it being in a centralized network. Another such scenario is Environmental problems or Animal protection. We can protect species that are endangered and animals that are suffering a similar health disease. Also, we will be able to address a lot of environmental problems by using DTNs and opportunistic networks. Like suggesting to the farmer what to produce based on soil quality, how much water is needed, fertilization of crops, etc.

DTN protocols are not a standardized approach yet and most people work on traditional internet but we can expect DTN routing and MANETs to be used extensively in the future and be one of the most advanced and safe networks that people can trust and be available on. Although these networks are currently used for emergency scenarios and cases where information is very sensitive. However, I believe that these networks will be used extensively in every field in the future.

Conclusion

In conclusion, I would like to say that DTN and networks are a new type of network as they differ from traditional networks in many ways. One way is that DTNs are decentralized networks and do not need an underlying architecture for passing the messages. In Ad-Hoc Networks we do not need to know the path between source and destinations as the topology keeps on changing due to mobile nodes. In this study, we extensively discussed about these kinds of networks and their advantages and challenges.

I believe that in the future these networks will be used in various fields as they have a huge potential because no company is monitoring the data or the data is not saved in any server. Nodes are mobile phones and cars that we use in our daily lives. These gadgets if used in networks can be very advantageous in any accident or destruction as the network is formed as and when needed. Also, these networks are self-healing and self-configured in any environment making them suitable in scenarios where human help cannot reach. Overall I learned a lot about MANETs and VANETs.

This study can be further processed by considering more protocols for evaluation or building a novel protocol considering any natural calamity situation in mind. We can create a novel protocol considering the terrain, localities, and network connectivities in the areas. When a network calamity occurs the networks available like wired or even wireless networks won’t work in many scenarios. In such cases, these networks will be very helpful in sending messages and saving a lot of lives.

Bibliography

[1] Boldrini, Chiara & Lee, Kyunghan & Önen, Melek & Ott, Jörg & Pagani, Elena. (2014). Opportunistic Networks. Computer Communications. 48. 10.1016/j.comcom.2014.04.007.

[2] Lilien L. Kamal Z. H. Bhuse V. Gupta A. (2006). Opportunistic Networks : The Concept and Research Challenges in Privacy and Security.Proc of the WSPWN, *140*, 134–147. 10.1007/978-0-387-71058-7_5

[3] Kurose, Jim. (2014). Information-centric networking: The evolution from circuits to packets to content. Computer Networks. 66. 112–120. 10.1016/j.comnet.2014.04.002.

[4] Ud Din, Ikram & Hassan, Suhaidi & Khan, Khurram & Guizani, Mohsen & Ghazali, Osman & Habbal, Adib. (2017). Caching in Information-Centric Networking: Strategies, Challenges, and Future Research Directions. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2017.2787609.

[5] Hajimirsadeghi, Mohammad & Mandayam, Narayan & Reznik, Alex. (2016). Joint Caching and Pricing Strategies for Popular Content in Information-Centric Networks.

[6] B. Nour, K. Sharif, F. Li and Y. Wang, "Security and Privacy Challenges in Information-Centric Wireless Internet of Things Networks" in IEEE Security & Privacy, vol. 18, no. 02, pp. 35-45, 2020. doi: 10.1109/MSEC.2019.2925337

[7] G. Zhang, B. Tang, X. Wang, and Y. Wu, An Optimal Cache Placement Strategy Based on Content Popularity in ContentCentric Network., Journal of Information and Computational Science 11:8 (2014) 27592769.

[8] S. Guo, H. Xie, and G. Shi, Collaborative forwarding and caching in content-centric networks., In International Conference on Research in Networking, pp. 41-55. Springer Berlin Heidelberg, 2012.

[9] Atif Ur Rehman, Muhammad & Ullah, Rehmat & Kim, Byung-Seo. (2019). NINQ: Name-Integrated Query Framework for Named-Data Networking of Things. Sensors. 19. 2906. 10.3390/s19132906.

[10] Ahmed, D.E.; Ibrahim, H.; Khalifa, O. Performance Evaluation of AODV, OLSR, and GRP for Transmitting Video Conferencing over MANETs. *Int. J. Comput. Sci. Inf. Secur.* **2020**, *18*, 45–51. [**Google Scholar**]

[11] Rasheed, Chaudhary Muhammad Asim & Gilani, Saira & Ajmal, Sana & Qayyum, Amir. (2017). Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications. 10.1007/978-981-10-3503-6_4.

[12] Rubinstein, M.G., Moraes, I.M., Campista, M.E.M., Costa, L.H.M.K., Duarte, O.C.M.B. (2006). A Survey on Wireless Ad Hoc Networks. In: Pujolle, G. (eds) Mobile and Wireless Communication Networks. MWCN 2006. IFIP The International Federation for Information Processing, vol 211. Springer, Boston, MA . https://doi.org/10.1007/978-0-387-34736-3_1

[13] Lu, Y.; Wen, W.; Igorevich, K.K.; Ren, P.; Zhang, H.; Duan, Y.; Zhu, H.; Zhang, P. UAV Ad Hoc Network Routing Algorithms in Space–Air–Ground Integrated Networks: Challenges and Directions. *Drones* **2023**, *7*, 448. https://doi.org/10.3390/drones7070448

[14] Banoth, Rajkumar & Narsimha, G.. (2016). Secure multipath routing and data transmission in MANET. International Journal of Networking and Virtual Organisations. 16. 236. 10.1504/IJNVO.2016.079178.

[15] Mechtri, Leila & Djemili Tolba, Fatiha & Ghanemi, Salim & Magoni, Damien. (2015). An IDS-based Self-healing Approach for MANET Survival. 10.1145/2816839.2816840.

[16] I. Jawhar, N. Mohamed and L. Zhang, "Inter-vehicular Communication Systems, Protocols and Middleware," *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*, Macau, China, 2010, pp. 282-287, doi: 10.1109/NAS.2010.49.

[17] A. Bohm, "State-of-the-art on network layer aspects for inter-vehicle communication", *Technical Report IDE0748*, June 2007.

[18] I. Jawhar and J. Wu, "Qos support in tdma-based mobile ad hoc networks" in The Journal of Computer Science and Technology (JCST), Springer, vol. 20, no. 6, pp. 797-910, November 2005.

[19] I. Jawhar and J. Wu, "Quality of service routing in mobile ad hoc networks" in Resource Management in Wireless Networking, Springer, Network Theory and Applications, vol. 16, pp. 365-400, 2005.

[20] E. Tikhonov, D. Schneps-Schneppe and D. Namiot, "Delay Tolerant Network protocols for an Expanding Network on a Railway," *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Sakheer, Bahrain, 2020, pp. 1-6, doi: 10.1109/3ICT51146.2020.9311960.

[21] Faheem, Arshiya & Hassan, Zohaib & Odarchenko, Roman & Khan, Muhammad Qasim & Zaman, Abnash & Ayub, Muhammad. (2019). New Technique of Social Aware Routing Protocols in Delay Tolerant Network. 1102-1106. 10.1109/UKRCON.2019.8879984.

[22] Vahdat, A. and Becker, D. (2000) Epidemic Routing for Partially Connected Ad Hoc Networks. Duke Univ., Durham, NC, Tech.Rep. CS-2000-06.

[23] Spyropoulos, T., Psounis, K., Raghavendra, C.S.: Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: Proceedings of ACM SIGCOMM 2005 - Workshop on Delay Tolerant Networking and Related Networks (WDTN-2005), Philadelphia, PA, USA, pp. 252-259 (2005)

[24] John Burgess, Brian Gallagher, David Jensen, and Brian Neil Levine. MaxProp: Routing for vehicle-based disruption-tolerant networks. In Proc. IEEE INFOCOM, April 2006.

[25] A. Doria, and O. Scheln. Probabilistic routing in intermittently connected networks. In Proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), 2003.

[26] Keränen, Ari & Ott, Jörg & Kärkkäinen, Teemu. (2009). The ONE simulator for DTN protocol evaluation. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). 55. 10.1145/1537614.1537683.