Using Ad Hoc Networking in Emergency Situations

Spreading information in an emergency situation to help both people in danger and the emergency services

Project Specification

Freddie Brown
u1716717

Supervisor: Dr. Matthew Leeke
Department of Computer Science
University of Warwick
2019-20

Abstract

During a disaster, it is often very difficult to communicate using our devices. Whether this be because infrastructure has been damaged, or there is too much traffic over networks. This can mean people feel isolated and makes it difficult for the emergency services to know the situation on the ground. This project aims to help ease this by creating emergency Ad-Hoc networks during times of emergency. Using hardware already found in the devices people carry around with them day-to-day, information can be passed from person to person and can be sent to the emergency services. It could help improve the efforts of the emergency services by giving them a better picture of an area, helping to use their resources more effectively. This lets them to save more lives.

Keywords: Bluetooth, Ad Hoc, MANET, Emergency, Disaster

Abbreviations

MANET - Mobile Ad Hoc Network
VM - Virtual Machine
BCS - British Computing Society
WSN - Wireless Sensor Network
AODV - Ad-Hoc On-Demand Distance Vector
DTN - Delay Tolerant Network
DAG - Directed Acyclic Graph

Contents

Chapter 1

Introduction

This project is about investigating the application of MANETs for use in emergency situations. This is a technology which lends itself to the low infrastructure needs of a disaster scenario. They can form networks dynamically with low overheads. As mentioned in the specification, these are very interesting in fluid situations where nodes move in and out of a network [1]. Although this is the main area of exploration for the project, there are other areas which are just as important which also need to be considered. A project such as this brings up issues such as data privacy, packet routing and taking actions to prolong the battery life of a device. These are all areas which will have a huge impact on the success of a project such as this.

1.1 Motivations

The modern world is highly connected through our telecommunications systems. These are used to connect people together. One important usage of this, is to quickly contact the emergency services. As discussed in the specification, during a disaster, such as the one seen in the 2017 hurricane in Puerto Rico, not having access to a form of communication can cause great harm to peoples lives. A study estimates that the lack of communications services in the aftermath of the hurricane contributed to an increase in mortality of 62% [2]. Remote areas were hurt most, being without cellular data services for up to 41 days. It can make it difficult for rescuers to know what is going on and how to intervene such that they can make a difference. This commonly leads to high cost and disruption. Also mentioned in the specification was Hurricane Katrina, in this scenario, high winds destroyed antennas highly damaged or destroyed [3], many of which belonged to belonged to cellular providers.

This illustrates the need to develop systems which help to ensure connectivity, even in challenging times. The United Nations voted, in June 2016, that internet access is a human right that should be protected [4]. This puts our current systems under the microscope and shows how important these services are to people and how access to them can save lives.

1.2 Project Aims

This project is aiming to develop a system which could be integrated into future mobile devices, which allows for the dissemination of emergency information in the event of a disaster. The project will look at the different ways which this can be implemented, what the challenges are that this problem presents as well as peripheral issues which were mentioned earlier.

1.3 Stakeholders

As mentioned in the specification, the stakeholders in this project are those which will benefit from a system such as this being implemented. Those who live in areas which are frequently affected by large scale emergencies will be the ones who will use this more often. Furthermore, the emergency services will benefit greatly from a project like this so they can maintain a clearer picture of what the situation on the ground its, and where their efforts will be most effectively utilised.

Chapter 2

Research

2.1 Related Work

Emergency networks are difficult to implement because of, in many cases, the damage to infrastructure that is caused in an emergency or the strain that puts on the existing infrastructure. Disasters can be difficult to deal with after they happen due to this degradation in communications infrastructure [5]. This can then hamper efforts to rescue survivors as they will struggle to communicate with those who need saving. Having a system in place, specially for this scenario, could save the lives of those that are affected by disaster [6].

An interesting attempt to solve this problem is HIRO-NET [7]. This system has 2 tiers: a local meshing using Bluetooth Low Energy (BLE) to connect devices together using a client-server model, and a way to connect together these local networks. In local meshing, a node starts off as a client and will try and find a server to connect to. After a while, it will timeout and will become a server for nodes to connect to. Doing this means that, when nodes join to network, over time it becomes easier to connections to form. Piconets are joined together to form Scatternets and packets are transported within them. If a Piconet has an active internet connection, the server will declare this. This means that other servers will route packets to this Piconet to be sent out over the active connection. This system is complex but allows for a more regular level of service for users.

A more simple approach then HIRO-NET has a greater focus on providing information for the emergency services [8, 9]. It takes some information, such as geographical information, and transports it to a central node to allow this information to be aggregated. The suggested systems use both WiFi and Bluetooth and how they can both play an important role together. These conclude that, as WiFi has a wider range and is more available, it plays a more important roles than Bluetooth. It also states that using WiFi Direct can provide a large speed boost when spreading information [9]. It means that a connection doesn't need to happen for a device to spread critical information about itself, which has obvious benefits for the types of situations that this project is investigating.

WiFi is an incredibly important technology as it supports long range transmission. For some standards, transmission can be up to, or close to, 1,000m in certain situations [10, 11]. Bluetooth tends to be used more for short range transmissions [12]. It relies on being in quite a well populated area as its range is limited. Each have their uses. Bluetooth is also considered to be more power efficient [13] than WiFi, but this is disputed for certain use cases [14]. This means it is sensible to consider both technologies for this project. This project is focusing on close range communications in environments where users may not have access to a stable power source. For this reason, Bluetooth may be a better choice than WiFi. WSN systems which use Bluetooth could provide an ideal model to analyse, such as [15]. This example discusses a high performance sensor network using highly optimised hardware. It presents an interesting model for nodes to work efficiently, such as only have 1 outgoing route for traffic. This could be applied in this project by only allowing a node to send data to 1 other node at any point.

A more recent, and very applicable, example of Ad Hoc networks is in the automotive industry. As cars have become more advanced, they have included more powerful computers on-board. Research has been done which looks into how they can be used to form networks made up of these vehicles. A number of studies [16–18] have investigated different aspects of this type of network. As discussed in [16], VANETs can communicate with each other as they drive past each other, communicating information between themselves. This information could be about similar things to the data in this project, such as location data of interesting events, like traffic jams. Although, as also discussed in [16], this isn't a stable network as they may be moving too fast to be able to communicate effectively. It offers a number of solutions, such as using store-and-forward routing algorithms or using Cellular data. VANETs also have a number of other issues similar to this project,security and routing. [17, 18] discuss a number of different possibilities for routing, such as novel ideas like geographical routing [18] and more established routing protocols such as AODV [17, 19] and how well they perform in this paradigm.

2.2 Security

Security is an area of this project which needs serious consideration. The legal and social ramifications [20] of ignoring it can be extremely high. As this project is dealing with sensitive location data, it is crucial that a solution is found that will ensure integrity and confidentiality. If it isnt́, data could be harvested and used to the detriment of those who survive a disaster. An example of post–disaster problems is looting, which was seen after Hurricane Katrina in 2005 [21].

Firstly, a method of sharing a key with the nodes is needed so they can encrypt information before it is transmitted. A way to accomplish this is to use Diffie–Hellman key exchange [22] so symmetric key encryption may be used. As suggested by [23], this protocol has issues with security and is susceptible to man in the middle attacks.

An alternative to using symmetric key encryption is using public key encryption, such as RSA [24]. In this, each member which wants to receive data will declare their public key, which is available to everybody. Once the message has been encrypted with the public key, only the private key can decrypt the message. As the private key should only be known by 1 users, this means only the correct recipient may view the encrypted data. This will provide messages with the confidentiality that is needed. To provide integrity to the messages, digital certificates could be used [22].

2.3 Routing

As Bluetooth uses a client-server model, routing is usually device-to-device. With this, it forms multiple small groups of devices (Piconets). These can be joined together and packets can be routed between them. Furthermore, other topologies which aren't as stable also exist, and so packet routing needs to be investigated in these forms too. By investigating all of these, a variety of circumstances can be covered.

As MANETs are already in use in a variety of situations, there are a couple of routing protocols that are already used. One popular one is AODV [19, 25], a combination of dynamic source routing and distance vector routing. This algorithm uses a series of packets to build routes, which are stored in nodes throughout the network. These are built using Route Request(RREQ) packets being broadcast across the network, flooding it. When an RREQ packet reaches the desired node, a Route Reply (RREP) packet is broadcast back, along the path which was used to reach the node in the first place. When an RREP packet is received by a packet which transmitted an RREQ packet, it creates a pointer in its routing table. This means it knows where to route any packets for that node in the future.

Another algorithm which is used for routing within MANETs is TORA [26], a type of routing algorithm that uses a DAG to determine which nodes to route packets through to the destination of the packet. If a node wants to route packets to a sink, F, it will broadcast QRY packets, which are relayed until it reaches a node adjacent to F. When it reaches these nodes, they broadcast a UPD packet which contains the id and distance from the sink node. These are propagated back towards the source node. This allows a graph to be constructed and allows routing to be done based on distance. The advantage of this method is that it has fewer control packets compared to other, similar methods as it only reacts when changes are discovered in the topology. Furthermore, partitions in the network are easily detected, whereas in AODV the source will send lots of RR packets which will flood the network.

An interesting are of packet routing, is swarm-based packet routing. It has been shown to perform better than a number of other, more established routing algorithms [27]. Swarm-based algorithms tend to find the best path in a network, but also include a probability that a different route will be chosen. As a MANET is an inherently unstable network, this is good as it allows new, better paths to be found. It also includes a time parameter to force information to be recalculated if it hasn't be used in a while. This feature also forces the exploration of new, quicker paths in the network. This type of routing is typical of a number of swarm-based routing algorithms, such as ant-colony routing [28].

An alternative type of biological routing is based on bees [29]. This protocol has a scouting stage where each node in the network is ścouted.́ Scout packets will be sent out to each neighbour and will travel through the whole network. They are passed on each time they visit a node until they reach a sink node. A back bee packet is then sent from this node towards the source. This process is done to evaluate the efficiency of routes between nodes. This is similar to the way that more established algorithms, such as AODV, work, except the scouting it much wider ranging, whereas in AODV, the equivalent stage is only done for 1 node at a time. This is a promising solution for MANETS, but the packet overhead might be too much for some time-sensitive cases.

The algorithms investigated already all look at algorithms which are only really useful in networks which are more stable. Connections are broken infrequently meaning the optimisations which have been discussed, can actually make a difference. Another form of routing caters more for networks which are less stable. Optimistic routing algorithms are common in DTNs and are good spreading information quickly. There are many different examples of this. One example of this is inspired by epidemiology to model how packets can flow through a network [30, 31]. It works by a node passing any information it has onto available neighbours. This is similar to how a disease might spread within a general population. Each node which receives these messages will store them and then carry them forward. If these nodes are physically moving, it allows packets to achieve large multi-hop movements with far fewer exchanges.

An alternative to disease-based routing, is to consider another type of routing also used within in DTNs, social-based routing [32]. This kind of routing considers the behaviours of nodes within a network. This will help improve the choices that a node makes as it considers the likelihood that the other node will forward the packets that it is going to transmit. It uses a group of set social characteristics to determine whether its behaviour is 'good' and cooperative or if its 'bad' and only caring about its own resources e.g only forwarding on messages from a select group of users. Other studies, such as [33, 34], show how powerful social-based routing protocols can be. They help to reduce the number of packets which are sent, and increase the probability that these packets actually are delivered. As can be seen in [34], the chance of delivery is lower than epidemic routing, but the number of packets which are sent is far lower and the latency is far greater. This could help to reduce traffic and unnecessary traffic in the network.

Chapter 3

Ethical, Social, Legal and Professional Issues

3.1 Ethical Issues

Ethical issues can come up when a project has a number of different objectives, each with negative effects which aren't immediately present. The benefits this objective could bring, if fulfilled, might out weight the immediate negatives for an objective and so due diligence on other impacts may be forgone. An example of this is in a project which collects lots of personal data. An objective of the product might be to increase cash flow of the company. Using this data to provide products such as targeted adverts may seen like a good idea at first, but might create some reputations damage in the long run. These kinds of issues may lead to data leaking or some people may find this an invasion of privacy. These damage had impacted Facebook recently. [35]. In this project, location data is used among a number of nodes. This data should be protected so that it can't be used for anything unintended by nodes which have access to it. This could be through encryption or forms of providing data privacy.

3.2 Social Issues

Social issues are those that have an affect on the lives of groups of people. As discussed in the project specification, these problems could affect how people interact with each other or could limit their access to certain goods and services. It may also relate to certain groups having access to key services over other, marginalised groups. It is difficult to see any of these issues relating to this project but this should be continually reviewed as the project moves onwards.

3.3 Legal Issues

A large part of this project is about sending sensitive data about vulnerable people, issues around data privacy need to be considered seriously. In this project, data is being sent to other devices nearby, so trust issues which may arise. To counter this, encryption could be used to provide data privacy. By doing this, it limits access only to users who should have access to the data. Otherwise, if this isn't protected, malevolent users may use it to cause harm to others, such as terrorists looking to find people to harm.

3.4 Professional Issues

As mentioned in the project specification, the project will adhere to the BCS Code of Conduct [36]. The aim of the project is to produce a research project which can be used in the future. This means adhering to these rules is very important. Furthermore, the project will pay close attention to the Research Code of Practice at the University of Warwick [37] and the departmental rules on ethical consent for any data the project may collect from participants in any potential testing [38].

Chapter 4

Project Requirements

4.1 Functional

FR1 - The system must use a widely used MAC layer protocol such as Bluetooth or WiFi.

FR2 - The system must use data privacy techniques, such as encryption, to prevent data falling into the wrong hands.

FR3 - The system could monitor battery life and make choices based on its predicted life expectancy

FR4 - The system could use a system of authentication to verify nodes, such as using a trust-based system or digital certificates

FR5 - The system must use the concept of sources and sinks, where sinks collect data and don't transmit information packets, and sources send and receive information from other sources.

FR6 - System must have a way to identify devices within the network. This ID should be used within packets sent by each device about themselves.

FR7 - Project could use a location discovery service such as GPS to get location data

4.2 Non-Functional

NFR1 - The system must be fully documented and maintainable. This means that the project is easily extensible and can easily be implemented on other platforms.

NFR2 - The system must be easy for a user to connect to and use. This is vital for the project as time is an important factor in an emergency situation and so the less time a user has to worry about how it works, the quicker they can use it to get help

NFR3 - The system must be created so it can be applied to a large population of devices. This project works optimally if there are a large number of devices to connect so design choices should consider the need for this project to work at a large scale.

NFR4 - The system must be able to be used by different types of devices such as Phones, Tablets and PCs. Much like **NFR3**, this project should be designed so it can be easily transported onto other devices so that they can also participate.

NFR5 - The system must use secure communications so bad actors cannot steal and weaponise the information.

NFR6 - System should require as little user interaction as possible to increase efficiency.

4.3 Constraints

As was discussed in the project specification, the project is constrained by the number of devices which it can be tested with. It is very expensive to test on a number of devices so, for that reason, the project will use a cheaper alternative, the Raspberry Pi. This will demonstrate the applications of this project, but can't replicate a proper use case of this project as it will lack the scale of devices which would be needed.

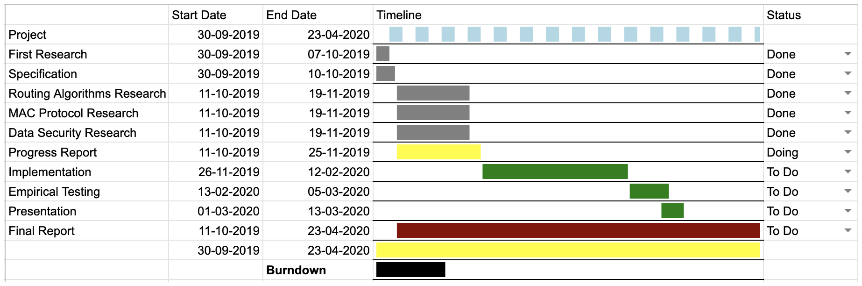
Another constraint is the types of devices, that can be used. The research will focus on applications in a heterogenous network of devices but it is likely this will only be demonstrated on a homogenous network as more popular devices (e.g iOS and Android [39]), which this type of system would be employed on in the real world, require separate development. This is outside of the scope of this project as it would require more time than is available to it. This would be a stretch goal for the project or could be considered a further extension for the future.

Chapter 5

Project Management

5.1 Project Timeline

As can be seen in fig.5.1, it shows the predicted project timeline in a Gantt chart as well as displaying the dates between which each task will take place. A large block of time has been left for the implementation of the project, about 2 months. This gives time for the project code to be written, tested and iterated on. This is to catch bugs and produce a working system. When this is complete, testing of the system will be done to look at the performance of the project so the project can be analysed. With all of this, a presentation will need to be produced. This will detail the different stages of the project, how the system works, as well as retrospectively looking at the project and discussing what went well and what could be improved in the future. With all of this produced, the final report will be written which will discuss all of this in further detail and will assess whether or not the project has been a success.



	Start Date	End Date	Timeline	Status
Project	30-09-2019	23-04-2020		
First Research	30-09-2019	07-10-2019		Done
Specification	30-09-2019	10-10-2019		Done
Routing Algorithms Research	11-10-2019	19-11-2019		Done
MAC Protocol Research	11-10-2019	19-11-2019		Done
Data Security Research	11-10-2019	19-11-2019		Done
Progress Report	11-10-2019	25-11-2019		Doing
Implementation	26-11-2019	12-02-2020		To Do
Empirical Testing	13-02-2020	05-03-2020		To Do
Presentation	01-03-2020	13-03-2020		To Do
Final Report	11-10-2019	23-04-2020		To Do
	30-09-2019	23-04-2020		
		Burndown		

Figure 5.1: Project Timeline

5.2 Project Tools

The project will use a variety of tools to accomplish its goals. The project will be written in **C/C++**. This is because its a low level language and it allows more fine grained control over aspects of the project. Along with this, **blueZ** will be used to interface with Bluetooth. This is a widely used library for projects such as this, with a number of resources to draw from [40].

In terms of hardware, as discussed in the project specification, the project is going to be written for Linux-based devices such as the Raspberry Pi which have Bluetooth on-board. Bluetooth is a common technology used by a number of devices, so is a useful medium to use for a project like this. Using a widely used technology increases the number of technologies that this project could apply to.

Other tools are needed to monitor the progress of the project. This project has been using **Trello** to keep track of tasks which need to be done and have been done. This is being used because its clear to use and allows tasks to be grouped clearly. Alongside this, **GitHub** has been used to backup code and keep track of project history, in case an older version of the project is needed. This is a widely used product in industry, so is a good choice for this project.

5.3 Risk Management

As mentioned in the project specification, this project doesn't have too many major risks that could have an effect on its performance. One risk, which was discussed above, is losing all physical machines which hold the project. This can be mitigated by storing any code and reports on Github, as well as maintaining a local copy on a hard drive. This provides extra layers of assurance that the project won't be lost.

Another risk is that persons who work on the project fall ill or are unable to do work. This can be mitigated by keeping in contact with DCS and discussing any factors that could lead to a delay in the projects completion because of this reason.

Furthermore, there is a risk that part of the project might overrun its planned length of time. This could be because hardware access has been delayed or there are extra technical difficulties that weren't foreseen during the planning of the project. Generous amounts of time have been allowed for each stage, as well as considerations within each stage. For example, in the implementation stage, there are different stages to development. The first stage is to complete basic functionality of the project before layering more features on top. This way of working means there will always be a working version of the project which meets the requirements.

Chapter 6

Progress

6.1 Defining Project Scope

The project specification focused on 2 directions for the project, it was quite broad. Since then, the scope of the project has been tightened so that the project is more focused on relevant goals.

One option for the project, which was discussed, was a project similar to HIRONET [7], a large network which used local bluetooth meshing to pass IP packets to devices, within a piconet/scatternet, which had atleast one active internet connection. With a system like this, routing protocols such as swarm-based routing algorithms [27–29] can also be used, enabling further improvements in network efficiency. Some of the benefits of this kind of system are:

- Creates a flexible network
- It is more useful to each survivor as they will have internet access; large variety of services to access
- More efficient data efficient; Doesn't constantly flood the network with packets
- Easy to implement 2-way communication between survivors and others; Can route packets to and from nodes as network is more stable

Although this proposal has a number of huge benefits, it also has a number of drawbacks:

- It is difficult to implement and probably beyond the reach of this timeframe. Too much complexity
- Difficult to use in a sparsely populated area; Less useful in many environments

- May need to use multiple different technologies to accomplish this on top of Bluetooth, such as Wifi. Adds to the already large complexity
- Server nodes need to do a lot of work, not good when aiming to conserve battery life

An alternative solution is to implement a solution akin to more common DTNs [8, 30, 32, 34], similar to a number of fault-tolerant networks. In this solution, as has been described before, messages about the status of survivors are passed between devices to a sink, usually the emergency services. These messages will contain location data about survivors which can be collected by the emergency services. The packet routing method will be one common to DTNs, either social-based or epidemiology-based. Some of the benefits of this are:

- Simple. Makes it easier to implement on a number of different devices so more nodes in the network
- Lightweight information. Reduces the packet size so data transmission is quicker
- Able to work effectively in both dense and sparse environments
- Network focused on emergency services, more beneficial to them
- Very tolerant to nodes coming in and out of the network
- Works well in topologies with lots of moving nodes

Like the first proposal, this also has some issues which have to be considered:

- Less efficient. Price of simplicity is that routing is more primitive and so less efficient
- 2-way communication is difficult because there is no constant network of devices with addressing
- More computation is involved: connections formed with other nodes more often, more nodes routing packets

After considering both of these ideas, the direction of the project will be the second proposal, utilising epidemic routing to build a fault-tolerant, lightweight network for spreading information among local, moving nodes. It has a more realistic implementation timetable and has a clearer and better defined use case.

6.2 Timetable

In the project specification, a timetable was defined which displayed the planned activities which were to be accomplished if the project is to be successful, as well as the dates which they need to be completed by. This was done to give the project structure and to help plan for deadlines. Since this part of the project was submitted, a few changes have been made, as can be seen in fig. 5.1. In this updated timetable, the time for improvements and testing have been rolled into the implementation period. This was done to be in line with principles of test driven development. Also, parts of the timetable have been marked as done. These parts of the project were to be completed in between the project specification and the progress report. These have been completed mostly, as well as some extra research into implementation and working out how the project will work.

6.3 Technical

As well as defining the project scope, work has been done on investigating the technical parts of the project, such as in defining what should be sent within the packets in the network. A principle of the packet structure for the project is that it needs to be small. This is so that as much data as possible can be fit inside as few Bluetooth packets [41] as possible. Only essential information should be included in the packet. Inspirations for a format are the FIX messaging protocol [42], a widely used protocol for transporting financial data, and JSON [43], a widely used data format in industry. The advantage of using a protocol like to FIX is that it has a number of security benefits. It uses a group of specified tags which describe very specific information. This means that a program will only analyse the data for specific tags which it cares about, which reduces the chance of unwanted information being processed. If extra functionality is added, nodes can ignore the extra data included, which allows for backwards compatibility in the future. On the otherside, JSON would be good as it is concise and very flexible. There is lots of support for it as it is very established. Both of these offer a lot of inspiration for a format of exchange to use.

The data to be included within packets has also been investigated. Obviously, including location data needs to be a priority. This can be done by using GPS, a common way of collecting location data. This is available on most devices today to power a number of location based applications. As well as this, an ID should be included in the packet. This will allow the sink to aggregate the data based on the device from which it originated. As well as this, including a timestamp saying when the packet was generated will allow the sink node to determine how old this data is. This way, it allows the emergency services to determine if the location data is accurate and allows nodes to prioritise which packets to forward first.

As well as considering packets, work has been done working towards understanding how the different libraries work. BlueZ [44] is a very useful, and widely used, library for C/C++ but has very little documentation. Much work has been done working towards understanding how it works. As it also contains a number of command line tools, BlueZ has a lot of open source code which uses a lot of the features which this project will use.

Chapter 7

Testing

As discussed in the specification, testing in this project will be used to verify the functionality of the project while changes are made as well as being able to verify that requirements have been fulfilled. The project will use different technologies to accomplish this. A unit testing framework will be used, such as **CUnit**, to test and verify the project. Also, other technologies will be utilised, such as bash scripting. This allows for tests to be written easily for a variety of projects and makes the testing process more flexible. For integration testing, **TravisCI** will be used. It is a robust service which is widely used and works very well with GitHub.

7.1 Unit Testing

A test will be written for each part of the project that is written to verify that it functions as it is needed to. Agile development methodologies will be adhered to by writing failing tests, which are then made to be passing by writing the code for which passes the test. Unit testing and its benefits are further discussed in [45, 46]. In these, they discuss the benefits of Test Driven Development and how unit testing works and is beneficial to a project. Unit testing is very useful and allows the functionality of the project to be verified quickly and easily.

7.2 Integration Testing

TravisCI allows larger tests to be written to incorporate more of the project. This is run on a clean VM which means there is nothing external to the project which could influence its testing. It enables more rigorous testing and fewer outside influences. This approach to testing the system is discussed in [45].

7.3 Success Management

Success for this project will defined by whether a network of Raspberry Pis, running the software written for this project, can pass packets about their location, between each other to a central repository node representing the emergency services. On top of this, there will be other measures of success for sub-targets, such as data privacy. These targets will be included in the requirements section of this report.

Chapter 8

Conclusion

Overall, the project has started smoothly. This part of the project plan has always been earmarked for research into the different areas which the project will touch on. At this stage, a good plan has been developed which will provide a structure for the project going forwards. Obviously, parts of the project will change with implementation, but this is acknowledged in this report. Much of the work which has been done so far has been to define a framework within which the implementation can be done. Being critical, this has been done to a good degree, but some extra work will have to be done during implementation. Not all libraries which will be used have been nailed down and, as a result, how an individual ID will be generated is not 100% certain yet. Over December, January and much of February, implementation will occur. The project is in a good place to start implementation. Some details are fluid still, but overall much has been nailed down and the majority of research has been completed.

Appendices

Appendix A

Using Ad Hoc Networking in Emergency Situations

Spreading information in an emergency situation to help both people in danger and the emergency services

Project Specification

Freddie Brown
u1716717

Supervisor: Dr. Matthew Leeke
Department of Computer Science
University of Warwick
2019-20

Abstract

During a disaster, it is often very difficult to communicate using our devices. Whether this be because infrastructure has been damaged, or there is too much traffic over networks. This can mean people feel isolated and makes it difficult for the emergency services to know the situation on the ground. This project aims to help ease this by creating emergency Ad-Hoc networks during times of emergency. Using hardware already found in the devices people carry around with them day-to-day, information can be passed from person to person and can be sent to the emergency services or out over an internet connection. It allows survivors of these kinds of situations to maintain contact with the rest of the world.

Keywords: Bluetooth, Ad Hoc, MANET, Emergency, Disaster

Abbreviations

MANET - Mobile Ad Hoc Network
VM - Virtual Machine
BCS - British Computing Society
WSN - Wireless Sensor Network
AODV - Ad-Hoc On-Demand Distance Vector
DTN - Delay Tolerant Network
LSR - Link-State Routing

Introduction

The main part of this project is investigating the application of MANETs for emergency situations, an interesting technology which could be used effectively for emergency situations. They are low infrastructure networks which use homogenous and heterogenous devices to form a network dynamically. This is incredibly interesting in situations which are quite fluid, with nodes coming in and out of a network [1]. There are some other areas which this project will also explore, such as keeping devices alive for a long time, biological inspired routing and security issues related to passing packets of potentially sensitive data to unverified devices to distribute. These areas complement the main project problem as they help to solve some questions associated with MANETs in this context.

Motivations

Today, most people in the world rely on telecommunications to connect with family members, friends, work colleagues and, very importantly, the emergency services. When we get a disaster, or group of them, as was seen in Puerto Rico in 2017, it can impact lives and even end them prematurely. A study estimates the increase in mortality of 62% [2], and this is thought to be an underestimate. Remote areas were hit hardest and were without services such as cellular data access for up to 41 days. This can make it very difficult for rescuers to know what's going on and how to intervene effectively. This is a common cause of high cost and disruption in many different disasters. Another example of this was after Hurricane Katrina [3] where high winds saw antennas, belonging to cellular providers, highly damaged or destroyed.

Incidents such as these illustrate the tragic consequences these events cause without vital services which are required nowadays. In 2016, the United Nations voted that access to the internet is a human right that should be protected [4]. This type of action brings into focus the need to have systems in place to help maintain connectivity, even when traditional infrastructure fails.

Project Aims

The aim of the project is to produce a prototype of a system which could be implemented by governments and technology companies which could help people. Companies like Google and Apple produce the Operating Systems for most phones [5] but they don't have any sort of inbuilt emergency system like the one I hope to accomplish.

I want to explore the different ways this could be implemented, what holds them back and how well they actually perform in action. Also, I want looking at why there is no widely implemented system such as this in consumer phones already.

Stakeholders

The stakeholders for this project would be those who can benefit from it. Those who live in areas which are frequently affected by natural disaster and have weak infrastructure, either as a result or because of lack of funding. These are the people that would benefit most from having a system which could help them maintain contact with the world if they can't through traditional methods.

Research

Different Implementations

A system such as this is difficult to implement, but could be of huge value. The aftermath of a disaster can be painful because of the lack of communications infrastructure [6]. This makes rescue efforts tough and makes people anxious whether their loved ones are alive. Having a way for devices to work together during this time could really enhance the lives of the people affected by disaster [7].

Although this is still an open problem, there have been a few different implementations and ideas about similar systems. One such example is HIRO-NET [8]. In this example, the approach looks at 2 tiers. One tier uses local meshing, similar to this project, and the other tier connects these mesh networks over a larger area. The local meshing uses Bluetooth Low Energy to connect devices together and sticks to a Client-Server model. Each server will start off as a client. If it cannot find any nearby server, it will then become a server and start advertising as such. If another server then appears, they will join together their piconets to form a scatternet to increase the number of connected devices. Servers declare if their piconet is connected to the internet so that other servers can route packets to it to send out beyond the local mesh. The main aim of this is to allow devices to maintain a regular internet connection to allow them access to normal internet services, such as social media. This could be important in a disaster scenario because they can often leave people isolated. Helping them to maintain access to services such as social media helps them to maintain that connection to the outside world.

Another approach focuses on getting emergency information out to the emergency services [9, 10]. This approach is a lot more simple than HIRO-NET as its sole focus is taking an emergency message, such as geographical information, and transporting it to an operational base to allow rescuers to find people who are in trouble. This proposed systems investigate the use of both WiFi and Bluetooth in an emergency communications system and how they can both play an important role together. The conclusion in this research is that, because WiFi has a longer range and is a more widely available technology, it plays a more important role than Bluetooth is spreading emergency information. Furthermore, using Wifi Direct to quickly transfer information to other devices nearby gives a large speed boost to spreading information, as proposed in [10]. This means no connection needs to occur and a device can spread critical information about itself to others. This is very useful in itself as it means the emergency services get data they need, quickly, so they can save lives.

WiFi is a very important and very useful technology because it is long-range. For example, 802.11p can reach up to 1,000m [11] whereas Bluetooth is typically used for shorter ranges. This is discussed in [12]. Using Bluetooth relies partly on being stuck in quite a populated area, due to its short range. This isn't always the case and so having another, longer range method of communication could be help connect isolated people over longer distances. Despite this, when there is a scenario where devices are going to be without a power source for a long time, it could be more power efficient to use Bluetooth [13], although some dispute this [14] so it is sensible to consider both technologies. For this reason, looking at Bluetooth WSN systems could provide inspiration for how to build the system. A system presented by [15] shows a high performance sensor network system. Although it uses highly optimised hardware to accomplish the task (which is different to the system this project is investigating), it presents ways for nodes to work more efficiently, such as only having 1 route to send outgoing traffic. It also presents how the WSN is formed and the role of each node. Each node powers itself, much like they would in an emergency situation, so have to be careful about using too much power.

Data Privacy

Data privacy is a necessary, important, and highly sensitive topic which has legal ramifications if ignored [16]. It is especially important in this project because it will deal with information which, if in the wrong hands, could harm someones wellbeing. For this to be effective, any solution needs to ensure confidentiality and integrity of the data. Someone could collect location data being broadcast by devices and could use it to see where the lowest density of people is so that they can loot abandoned houses. Looting was a big problem in the aftermath of Hurricane Katrina in 2005 [17].

One way to do this might be to use Diffie–Hellman key exchange [18, 19] alongside another symmetric key algorithm, which provides confidentiality. DH is a well known way to do public key exchange over a public, interceptable channel like bluetooth. There are some drawbacks to this, such as user authentication, as presented in [18]. This could be solved by using a digital certificate. This is discussed in [19]. It proves the integrity of a message which is sent as it can't be replicated by a 3rd party. Another positive to this is that there doesn't need to be any keys stored over a long period of time. This reduces vulnerability to attack and makes solving each key by brute force a less attractive prospect. On the other hand, calculating keys each time can be a computationally intensive process. It could waste valuable computational power, especially when there is a serious motivation to conserve power and use resources as effectively as possible.

Further options could include using public key encryption, such as RSA [20]. This is a highly secure method and is widely used in industry. In a MANET, each node could broadcast its public key when it connects to the network as an update. Each node could store this public key. Every time a node wants to communicate with another node, it can encrypt the message with the receiving nodes public key. This way the privacy of the message is maintained. To maintain integrity of the message, a digital signature could be used. The issue here is that there is a worry that unsolicited messages could be sent from nefarious parties with valid digital certificates to nodes. This could trick them into accepting the message and performing actions which work against other users in the network. This is a very pressing issue as users of the network are facing life or death situations. A way to counteract this may be to use a trust-based scheme to authenticate legitimate traffic [21]. This enables nodes to route and accept packets based on how much they trust another node. This could be a powerful tool and helps protect against replay attacks and other packet forwarding attacks.

Routing

Due to the Client-Server model employed by Bluetooth systems, routing tends to be device to device. For this project, it will investigate connecting multiple piconets together and routing packets between devices within a wider scatternet effectively. A good way to do this could be by using one of the many routing algorithms out there. An interesting area in routing is biological-inspired routing which is based on the behaviours of, usually swam based, creatures in the wild. This project is mainly looking at scenarios where nodes aren't necessarily predictable and fixed. For this reason, other types of routing need to be considered do deal with the unique circumstances people could find themselves in.

One particular area of routing is swarm based packet routing. This has been explored and is shown to perform better than a number of other routing algorithms [22], such as ones based on ant colonies. A number of the algorithms such as AODV routing are very popular in MANETs similar to the one proposed in this project. Part of the reason why this is a good solution for MANETs is because the path which will likely be chosen is the one which has been proven to have been the quickest. This means the probability the shortest path is chosen increases. There is a time parameter to this algorithm meaning that if a path isn't taken for a while, the influence of that path wanes. This means that new, faster routes have a good chance at being discovered quickly. As can be seen from the data presented in [22], it shows that this algorithm performs better than a number of established others. In this project, routing such as this could be useful. Adding an element of random discovery by using probability to select the route to take means that other routes can be discovered. As it is likely that the topology will change quickly. This could, overall, make the routing of packets more efficient as other paths will be discovered quickly.

As well as considering ant colony routing, there are other types of swarm based routing based on different principles in Biology [23]. Another version is based on Bees [24]. In this algorithm, bees do scouting of other nodes. Scouts will be sent out to each neighbour node. They travel through the network and are passed on each time until they reach a sink node. From this node, a back bee packet is sent back to the source. This is done to make an evaluation on the efficiency of the route between nodes. This is also a promising algorithm but could be troublesome considering there is a scouting stage. In the application of this project, this could take up time and power needed to send out packets to other nodes as this is a time sensitive use case.

An alternative avenue for routing in the network is based on the spread of disease. This form of routing is used in a number of DTN projects as it is good for optimistically spreading information quickly [25]. When a node realises it has neighbours, it sends all stored packets to them, as well as any packets it wants to send. This is done to increase the number of nodes which have been given all of the information it has. This is a similar way to how a disease spreads, it can only spread by coming into contact with another living being and is passed on by some sort of transport vector. In this case, that vector is a packet. This is a very quick way of spreading information but the criticism of this is the number of different packet exchanges which need to occur to spread the same packet. This makes the network quite computationally inefficient as the same computation has to be repeated over and over again in multiple nodes. But, it is good for networks which are temporary. This means it could work well in an emergency MANET similar to the one this project is proposing.

Aside from the different biological algorithms proposed above, there are a number of other different types of routing. One which has already been mentioned is AODV [26]. In this algorithm, routes in the network are built by a node flooding a network with request messages than using the route suggested by the quickest route reply message. Another class of routing algorithms that could also be used is LSR. This is used by the TCP/IP. There have been other optimised versions of this since, such as optimised LSR protocol [27]. This aims to improve on the performance of the established LSR protocol by reducing the number of nodes which control information is sent to by choosing which nodes to re-send control traffic to more selectively. Also, a node doesn't need to know as much of the topology than it does for LSR, only that of nodes it will use to re-send control traffic and what links they have.

Ethical, Social, Legal and Professional Issues

Ethical Issues

Ethical issues arise when there are competing objectives where some have unclear negatives. An example of this is using data collected through using a product to target certain groups without their consent. A firm may make more money by doing this, but whether it is right to do so is something that should be considered. Fundamentally, stakeholders in the project should be protected and their data shouldn't be used against them. Data should be kept anonymous and protected somehow, through traditional encryption or other means.

Social Issues

Social issues are those that may have an affect on the lives of many people. It could be problems which affect how they interact with other people or those relating to access to goods and services that others can but they can't. Currently, it is hard to see any issues of this nature relating to the project but this should be continually considered as the project moves forward.

Legal Issues

This project will deal with sending data about an individual to others and allowing them to hold and send this data to whomever they wish to send it to. There are legal issues as, without proper protections, this kind of data could be used against individuals that are in trouble, such as in a terror incident.

In this project, sensitive data will be dealt with appropriately, such as location data, so no one is privy to this information at any time if they shouldn't have access to it. As discussed above in Ethical Issues, this should be done by maintaining data privacy through encryption or other means.

Professional Issues

This project will adhere to the BCS Code of Conduct [28]. The aim is to produce a research project which can be trusted and respected and so adherence to all rules that are required is important. This means I will also follow the Research Code of Practice at the University of Warwick [29]. This means all work I use to support my research will be referenced.

Project Requirements

Functional

FR1 - The system must use a widely used MAC layer protocol such as Bluetooth or WiFi.

FR2 - The system must have the capability to have nodes connected to the internet (sinks) as well as those which aren't (sources/routers).

FR2.1 - Within the nodes not connected to the internet, there should be 2 types of node: Nodes of regular citizens(sources) and those belonging to the emergency services which can accept and deal with data like internet nodes (sinks).

FR3 - The system must use a mechanism to enable data privacy within packets, such as encryption.

FR4 - The system should consider the battery life and make choices to extend this as much as possible.

FR5 - The system could provide an API which can be implemented by other services.

FR5.1 - This API must be simple to use so services can route traffic in disaster scenarios.

FR6 - The system must use a mechanism to provide authentication of nodes in the network, such as using a trust-based scheme or digital certificates.

Non-Functional

NFR1 - The system must be fully documented and maintainable. This means that the project is easily extensible and can easily be implemented on other platforms.

NFR2 - The system must be easy for a user to connect to and use. This is vital for the project as time is an important factor in an emergency situation and so the less time a user has to worry about how it works, the quicker they can use it to get help

NFR3 - The system must be created so it can be applied to a large population of devices. This project works optimally if there are a large number of devices to connect so design choices should consider the need for this project to work at a large scale.

NFR4 - The system must be able to be used by different types of devices such as Phones, Tablets and PCs. Much like **NFR3**, this project should be designed so it can be easily transported onto other devices so that they can also participate.

NFR5 - The system could provide a way for other services to use the network to send out internet traffic. This makes the system more extensible. If other services, such as Twitter, wanted to implement features using this, it would increase usage of the system hugely as these services are very popular in a disaster scenario.

NFR6 - The system must make sure communicating between devices is secure. This is so bad actors can't harness peoples personal information against them.

Constraints

This project will be constrained by the number of devices which it can be tested on and the type of devices which can be used. Having access to lots of devices can be very expensive. This project will use Raspberry Pi's to demonstrate the application of the research but these cost money and it won't be able to replicate the scale at which an emergency situation may be.

A further constraint will be the types of devices. The research will focus on applications in a heterogenous network of devices but it is likely this will only be demonstrated on a homogenous network as more popular devices (e.g iOS and Android [5]), which this type of system would be employed on in the real world, don't allow root access and are restrictive about what can be run on devices. This makes them difficult to develop for on this project, but are platforms which this would need be implemented on in the real world.

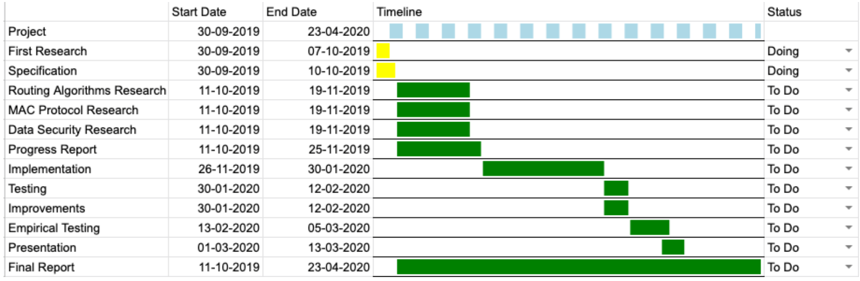
Project Management

Project Timeline

As can be seen in fig.1, it shows the predicted project timeline in a Gantt chart as well as displaying the dates between which each task will take place. Looking at the timeline, ample time has been left for research for the different aspects of the project (about a month). During this time, the second project deliverable can also be written. After this, a large block of time has been left for the implementation of the project, about 2 months. After this, a period of product testing and iteration has been scheduled so that bugs and improvements can be made so it performs better. After this, further testing will take place where results of the performance of the project can be collected so they can be presented in the final report and presentation.

Project Tools

This project will use C++ for programming. This has been chosen because it is a low level programming language so the code will be easier to optimise for increased performance. A library which will be used to interface with Bluetooth with is BlueZ [30]. This will provide a good api to interface with Bluetooth with on Linux machines.



	Start Date	End Date	Timeline	Status
Project	30-09-2019	23-04-2020	▨	
First Research	30-09-2019	07-10-2019	🟨	Doing
Specification	30-09-2019	10-10-2019	🟨	Doing
Routing Algorithms Research	11-10-2019	19-11-2019	🟩	To Do
MAC Protocol Research	11-10-2019	19-11-2019	🟩	To Do
Data Security Research	11-10-2019	19-11-2019	🟩	To Do
Progress Report	11-10-2019	25-11-2019	🟩	To Do
Implementation	26-11-2019	30-01-2020	🟩	To Do
Testing	30-01-2020	12-02-2020	🟩	To Do
Improvements	30-01-2020	12-02-2020	🟩	To Do
Empirical Testing	13-02-2020	05-03-2020	🟩	To Do
Presentation	01-03-2020	13-03-2020	🟩	To Do
Final Report	11-10-2019	23-04-2020	🟩	To Do

Figure 1: Project Timeline

In terms of hardware, the project is going to be written for Linux-based devices such as the Raspberry Pi which have Bluetooth. This is a pretty basic requirement for the hardware as Bluetooth is standard on a lot of devices. Having very few requirements lowers barrier to entry to use the project and makes it easier to see how it could be used on a variety of devices.

A variety of other tools will be used for other aspects of the project. Trello will be used to keep track of tasks that need to be done. This is a simple and clear way to see what it left to do and allows deadlines to be built into tasks. It also fits in with an Agile development methodology, which is preferable. On top of this, Git and Github will be used as the version control system to store code. It makes it easier to access project resources from multiple locations and provides a good back up if something went wrong and all physical devices which hold the project, were to break for some unforeseen reason.

Risk Management

In this project, there aren't too many major risks that could have an effect on its performance. One risk, which was discussed above, is losing all physical machines which hold the project. This can be mitigated by storing any code and reports on Github, as well as maintaining a local copy on a hard drive. This provides extra layers of assurance that the project won't be lost.

Another risk is that persons who work on the project fall ill or are unable to do work. This can be mitigated by keeping in contact with DCS and discussing any factors that could lead to a delay in the projects completion because of this reason.

Furthermore, there is always a risk that something might take longer than it is planned for to complete. This could be because hardware access has been delayed or there are extra technical difficulties that weren't foreseen during the planning of the project. Because of this, generous allowances have been made for each task in the project. If something finishes earlier than planned, other tasks can use this time. Also, if a task is running late, subsequent tasks have extra time built in to accommodate for any delays.

Testing

Testing in this project will be used to verify the functionality of the project while changes are made as well as being able to verify that requirements have been fulfilled. The project will use a couple of different technologies to accomplish this. For unit testing an established C++-specific framework will be used, such as CppUnit. For integration testing, TravisCI will be used. Once more, its a robust service and it has very good integration with Github and is very customisable.

Unit Testing

With unit testing, tests will be written for each feature that is created. These will be lined up with the requirements so that it is easy to see that they are being fulfilled. For writing unit tests, Agile development methodologies will be adhered to by writing the tests before writing the feature. Unit testing and its benefits are further discussed in [31, 32]. In these, they discuss the benefits of Test Driven Development and how unit testing works and is beneficial to a project.

Integration Testing

By using TravisCI, larger tests can be written which incorporated more of the project. This can be run on a clean VM which means there is nothing external to the project which could influence its testing. This enables more rigorous testing. This approach to testing the system is discussed in [31].

Success Management

The way success of the project can be measured is if the project can transmit packets across a group of devices with to a target device. This would simulate a device in a disaster scenario which is either the emergency services or an internet connected device. This will be tested on a number of topologies and in different environments to test performance when taking in lots of different physical and real world factors.

Conclusion

Overall the project has begun well. The tools which are going to be used are coming into shape and there is a greater understanding about what needs to be done in terms of further research and future implementation. Over the next few weeks, a greater plan of what needs to be done will be created and more cards for Trello will be made so that the project stays on track. Proper research will begin and a more rigorous plan will be devised so that it can be presented during the progress report. Throughout this specification, there have been a couple of areas in which there are multiple avenues that the project could take, such as in routing. Over the next few weeks of research, this will be cleared up so that this can be incorporated into the plan. The project will then be in a good place to start implementation.

Bibliography

[1] J.-Z. Sun, "Mobile ad hoc networking: an essential technology for pervasive computing," in *2001 International Conferences on Info-Tech and Info-Net. Proceedings (Cat. No. 01EX479)*, vol. 3. IEEE, 2001, pp. 316–321.

[2] N. Kishore, D. Marqués, A. Mahmud, M. V. Kiang, I. Rodriguez, A. Fuller, P. Ebner, C. Sorensen, F. Racy, J. Lemery *et al.*, "Mortality in puerto rico after hurricane maria," *New England journal of medicine*, vol. 379, no. 2, pp. 162–170, 2018.

[3] K. Banipal, "Strategic approach to disaster management: lessons learned from hurricane katrina," *Disaster Prevention and Management: An International Journal*, vol. 15, no. 3, pp. 484–494, 2006.

[4] H. R. Council, "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development," *UN General Assembly*, vol. A/HRC/32/L.20, June 2018.

[5] A. Holst, "Global mobile os market share in sales to end users from 1st quarter 2009 to 2nd quarter 2018." [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[6] B. Allyn and J. Beaubien, "Getting aid to bahamas is a logistical nightmare as support systems 'do not exist'." [Online]. Available: https://www.npr.org/2019/09/10/759431554/getting-aid-to-bahamas-a-logistical-nightmare-as-support-systems-do-not-exist?t=1570629766473

[7] T. Frank, "Cell phone service must be restored quicker after hurricanes." [Online]. Available: https://www.scientificamerican.com/article/cell-phone-service-must-be-restored-quicker-after-hurricanes/

[8] L. Ferranti, S. D'Oro, L. Bonati, E. Demirors, F. Cuomo, and T. Melodia, "Hiro-net: Self-organized robotic mesh networking for internet sharing in disaster scenarios," in *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2019, pp. 1–9.

[9] X. Wu, M. Mazurowski, Z. Chen, and N. Meratnia, "Emergency message dissemination system for smartphones during natural disasters," in *2011 11th International Conference on ITS Telecommunications.* IEEE, 2011, pp. 258–263.

[10] A. A. Shahin and M. Younis, "Alert dissemination protocol using service discovery in wi-fi direct," in *2015 IEEE International Conference on Communications (ICC).* IEEE, 2015, pp. 7018–7023.

[11] A. M. Abdelgader and W. Lenan, "The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges," in *Proceedings of the world congress on engineering and computer science*, vol. 2, 2014, pp. 22–24.

[12] P. Bhagwat, "Bluetooth: technology for short-range wireless apps," *IEEE Internet Computing*, vol. 5, no. 3, pp. 96–103, 2001.

[13] G. D. Putra, A. R. Pratama, A. Lazovik, and M. Aiello, "Comparison of energy consumption in wi-fi and bluetooth communication in a smart building," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 2017, pp. 1–6.

[14] R. Friedman, A. Kogan, and Y. Krivolapov, "On power and throughput tradeoffs of wifi and bluetooth in smartphones," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1363–1376, 2012.

[15] H. Chu, Z. Xie, Y. Shao, Q. Liu, and Z. Mi, "Design and implement of wsn based on bluetooth and embedded system," in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 5. IEEE, 2010, pp. V5–641.

[16] BBC, "Facebook to pay record $5bn to settle privacy concerns." [Online]. Available: https://www.bbc.co.uk/news/business-49099364

[17] A. Press, "Looters take advantage of new orleans mess." [Online]. Available: http://www.nbcnews.com/id/9131493/ns/us_news-katrina_the_long_road_back/t/looters-take-advantage-new-orleans-mess/#.XZus_CV7lTY

[18] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4. IEEE, 2010, pp. V4–634.

[19] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[20] F. J. Aufa, A. Affandi *et al.*, "Security system analysis in combination method: Rsa encryption and digital signature algorithm," in *2018 4th International Conference on Science and Technology (ICST).* IEEE, 2018, pp. 1–5.

[21] S. N. Shah and R. H. Jhaveri, "A trust-based scheme against packet dropping attacks in manets," in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. IEEE, 2016, pp. 68–75.

[22] T. L. Lin, Y. S. Chen, and H. Y. Chang, "Performance evaluations of an ant colony optimization routing algorithm for wireless sensor networks," in *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2014, pp. 690–693.

[23] G. Sharvani, N. Cauvery, and T. Rangaswamy, "Different types of swarm intelligence algorithm for routing," in *2009 International Conference on Advances in Recent Technologies in Communication and Computing*. IEEE, 2009, pp. 604–609.

[24] A. V. Leonov, "Modeling of bio-inspired algorithms anthocnet and beeadhoc for flying ad hoc networks (fanets)," in *2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, vol. 2. IEEE, 2016, pp. 90–99.

[25] T. Choksatid, W. Narongkhachavana, and S. Prabhavat, "An efficient spreading epidemic routing for delay-tolerant network," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 473–476.

[26] N. H. Phong and M.-K. Kim, "Enhancing reliability on wireless sensor network by aodv-er routing protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 6. IEEE, 2010, pp. V6–32.

[27] T. H. Clausen and P. Jacquet, "Optimized link state routing protocol (olsrp)," *The Internet Engineering Task Force, MANET working Group*, vol. 3626, 10 2003.

[28] "British computer society code of conduct," British Computing Society, BCS The Chartered Institute for IT, First Floor Block D, North Star House, North Star Avenue, Swindon, SN2 1FA. [Online]. Available: https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/

[29] "Research code of practice," Univeristy of Warwick, University of Warwick, Warwickshire, CV4 7AL, United Kingdom. [Online]. Available: https://www.warwick.ac.uk/services/ris/research_integrity/code_of_practice_and_policies/research_code_of_practice/

[30] "Bluez: Official linux bluetooth protocol stack." [Online]. Available: www.bluez.org

[31] R. Pressman, *Software Engineering: A Practitioners Approach 7th Edition*. McGraw-Hill, 2010.

[32] I. Sommerville, *Software Engineering Ninth Edition*. Addison-Wesley, 2011.

Bibliography

[1] J.-Z. Sun, "Mobile ad hoc networking: an essential technology for pervasive computing," in *2001 International Conferences on Info-Tech and Info-Net. Proceedings (Cat. No. 01EX479)*, vol. 3. IEEE, 2001, pp. 316–321.

[2] N. Kishore, D. Marqués, A. Mahmud, M. V. Kiang, I. Rodriguez, A. Fuller, P. Ebner, C. Sorensen, F. Racy, J. Lemery *et al.*, "Mortality in puerto rico after hurricane maria," *New England journal of medicine*, vol. 379, no. 2, pp. 162–170, 2018.

[3] K. Banipal, "Strategic approach to disaster management: lessons learned from hurricane katrina," *Disaster Prevention and Management: An International Journal*, vol. 15, no. 3, pp. 484–494, 2006.

[4] H. R. Council, "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development," *UN General Assembly*, vol. A/HRC/32/L.20, June 2018.

[5] B. Allyn and J. Beaubien, "Getting aid to bahamas is a logistical nightmare as support systems 'do not exist'." [Online]. Available: https://www.npr.org/2019/09/10/759431554/getting-aid-to-bahamas-a-logistical-nightmare-as-support-systems-do-not-exist?t=1570629766473

[6] T. Frank, "Cell phone service must be restored quicker after hurricanes." [Online]. Available: https://www.scientificamerican.com/article/cell-phone-service-must-be-restored-quicker-after-hurricanes/

[7] L. Ferranti, S. D'Oro, L. Bonati, E. Demirors, F. Cuomo, and T. Melodia, "Hiro-net: Self-organized robotic mesh networking for internet sharing in disaster scenarios," in *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2019, pp. 1–9.

[8] X. Wu, M. Mazurowski, Z. Chen, and N. Meratnia, "Emergency message dissemination system for smartphones during natural disasters," in *2011 11th International Conference on ITS Telecommunications*. IEEE, 2011, pp. 258–263.

[9] A. A. Shahin and M. Younis, "Alert dissemination protocol using service discovery in wi-fi direct," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7018–7023.

[10] W. Sun, M. Choi, and S. Choi, "Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz," *Journal of ICT Standardization*, vol. 1, no. 1, pp. 83–108, 2013.

[11] A. M. Abdelgader and W. Lenan, "The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges," in *Proceedings of the world congress on engineering and computer science*, vol. 2, 2014, pp. 22–24.

[12] P. Bhagwat, "Bluetooth: technology for short-range wireless apps," *IEEE Internet Computing*, vol. 5, no. 3, pp. 96–103, 2001.

[13] G. D. Putra, A. R. Pratama, A. Lazovik, and M. Aiello, "Comparison of energy consumption in wi-fi and bluetooth communication in a smart building," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2017, pp. 1–6.

[14] R. Friedman, A. Kogan, and Y. Krivolapov, "On power and throughput tradeoffs of wifi and bluetooth in smartphones," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1363–1376, 2012.

[15] H. Chu, Z. Xie, Y. Shao, Q. Liu, and Z. Mi, "Design and implement of wsn based on bluetooth and embedded system," in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 5. IEEE, 2010, pp. V5–641.

[16] B. Zheng, P. Wang, F. Liu, and C. Wang, "Cooperative data delivery in sparse cellular-vanet networks," in *2016 6th International Conference on Digital Home (ICDH)*. IEEE, 2016, pp. 128–132.

[17] H. Kaur *et al.*, "Analysis of vanet geographic routing protocols on real city map," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017, pp. 895–899.

[18] S. Hu, Y. Jia, and C. She, "Performance analysis of vanet routing protocols and implementation of a vanet terminal," in *2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC)*. IEEE, 2017, pp. 1248–1252.

[19] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*. IEEE, 1999, pp. 90–100.

[20] BBC, "Facebook to pay record $5bn to settle privacy concerns." [Online]. Available: https://www.bbc.co.uk/news/business-49099364

[21] A. Press, “Looters take advantage of new orleans mess.” [Online]. Available: http://www.nbcnews.com/id/9131493/ns/us_news-katrina_the_long_road_back/t/looters-take-advantage-new-orleans-mess/#.XZus_CV7lTY

[22] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[23] N. Li, “Research on diffie-hellman key exchange protocol,” in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4. IEEE, 2010, pp. V4–634.

[24] F. J. Aufa, A. Affandi *et al.*, “Security system analysis in combination method: Rsa encryption and digital signature algorithm,” in *2018 4th International Conference on Science and Technology (ICST)*. IEEE, 2018, pp. 1–5.

[25] N. H. Phong and M.-K. Kim, “Enhancing reliability on wireless sensor network by aodv-er routing protocol,” in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 6. IEEE, 2010, pp. V6–32.

[26] V. D. Park and M. S. Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks,” in *Proceedings of INFOCOM’97*, vol. 3. IEEE, 1997, pp. 1405–1413.

[27] T. L. Lin, Y. S. Chen, and H. Y. Chang, “Performance evaluations of an ant colony optimization routing algorithm for wireless sensor networks,” in *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2014, pp. 690–693.

[28] G. Sharvani, N. Cauvery, and T. Rangaswamy, “Different types of swarm intelligence algorithm for routing,” in *2009 International Conference on Advances in Recent Technologies in Communication and Computing*. IEEE, 2009, pp. 604–609.

[29] A. V. Leonov, “Modeling of bio-inspired algorithms anthocnet and beeadhoc for flying ad hoc networks (fanets),” in *2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, vol. 2. IEEE, 2016, pp. 90–99.

[30] T. Choksatid, W. Narongkhachavana, and S. Prabhavat, “An efficient spreading epidemic routing for delay-tolerant network,” in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 473–476.

[31] C. S. De Abreu and R. M. Salles, “Modeling message diffusion in epidemical dtn,” *Ad Hoc Networks*, vol. 16, pp. 197–209, 2014.

[32] Y. Zhu, B. Xu, X. Shi, and Y. Wang, “A survey of social-based routing in delay tolerant networks: Positive and negative social effects,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 387–401, 2012.

[33] G. K. Wong, Y. Chang, X. Jia, K. H. Wong, and W.-Y. Hui, “Performance evaluation of social relation opportunistic routing in dynamic social networks,” in *2015 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2015, pp. 874–878.

[34] Z. Zhu, S. Liu, S. Du, X. Lin, and H. Zhu, “Relative interpersonal-influence-aware routing in buffer constrained delay-tolerant networks,” in *2013 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2013, pp. 4446–4451.

[35] N. Patel, “It’s time to break up facebook.” [Online]. Available: https://www.theverge.com/2018/9/4/17816572/tim-wu-facebook-regulation-interview-curse-of-bigness-antitrust

[36] “British computer society code of conduct,” British Computing Society, BCS The Chartered Institute for IT, First Floor Block D, North Star House, North Star Avenue, Swindon, SN2 1FA. [Online]. Available: https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/

[37] “Research code of practice,” Univeristy of Warwick, University of Warwick, Warwickshire, CV4 7AL, United Kingdom. [Online]. Available: https://www.warwick.ac.uk/services/ris/research_integrity/code_of_practice_and_policies/research_code_of_practice/

[38] “Ethical consent,” Department of Computer Science, University of Warwick, Warwickshire, CV4 7AL, United Kingdom. [Online]. Available: https://warwick.ac.uk/fac/sci/dcs/teaching/ethics

[39] A. Holst, “Global mobile os market share in sales to end users from 1st quarter 2009 to 2nd quarter 2018.” [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[40] A. S. Huang and L. Rudolph, *Bluetooth essentials for programmers*. Cambridge University Press, 2007.

[41] MICROCHIP, “Bluetooth® low energy packet types.” [Online]. Available: https://microchipdeveloper.com/wireless:ble-link-layer-packet-types

[42] “Fix 4.2 protocol specification guide,” London Stock Exchange Group.

[43] D. Crockford, “Introducing json.” [Online]. Available: https://json.org/

[44] “Bluez: Official linux bluetooth protocol stack.” [Online]. Available: www.bluez.org

[45] R. Pressman, *Software Engineering: A Practitioner’s Approach 7th Edition*. McGraw-Hill, 2010.

[46] I. Sommerville, *Software Engineering Ninth Edition*. Addison-Wesley, 2011.