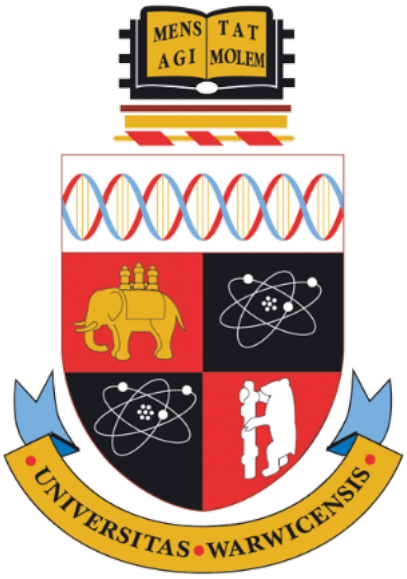

Using Ad Hoc Networking in Emergency Situations

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 collegues 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 disrupsion in many different disasters. Another example of this was after Hurricane Katrina [3] where high winds saw antennas, belonging to celluar 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 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

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 [5]. 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 [6, 7]. 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 [7]. 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 [8] whereas Bluetooth is typically used for shorter ranges. This is discussed in [9]. 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 [10], although some dispute this [11] 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 [12] 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. 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. Furthermore, during the emergency situations which this project is investigating, there are many nefarious actors which may want to harm people. If this was used during a terrorist attack, for example, data would need to be protected as it could alert bad actors to the locations of survivors and, as a result, could endanger their wellbeing. Furthermore, 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 Hurrican Katrina in 2005 [13].

One way to do this might be to use Diffie–Hellman key exchange [14,15] alongisde 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 [14]. This could be solved by using a digital certificate. This is discussed in [15]. 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 [16]. 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. Everytime 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 [17]. 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 [18], 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 [18], 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 [19]. Another version is based on Bees [20]. 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 efficency 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 [21]. 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 simialar 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 inefficent 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 [22]. In this algorithm, routes in the network are built by a node flooding a network with request messages then 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 [23]. 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 [24]. 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 [25]. 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 [26]), 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

The above figure 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 [27]. 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 unforseen 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. Thish 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 forseen 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 accomodate 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 [28, 29]. In these, they discuss the benefits of Test Driven Development and how unit testing works and is beenficial 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 rigourous testing. This approach to testing the system is discussed in [28].

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 rigourous 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] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] A. V. Leonov, "Modeling of bio-inspired algorithms anthocnet and beead-hoc 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.

[21] 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.

[22] 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.

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

[24] "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/

[25] "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/

[26] 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/

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

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

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