**UNIVERSITY OF MORATUWA**

Faculty of Engineering



GPA Module EN3992 – Project

**Wi-Fi Direct for Vehicle-to-Vehicle Communication: An Experimental Study**

120415V Nanayakkara N.P.

120459H Perera B.A.V.

120631E Siriwardhana M.A.A.S.

120700P Welagedara T.D.

Supervisor: Dr. Tharaka Samarasinghe

Date of Submission: 21/10/2016

Contents

[1 Problem Statement 3](#_Toc464824179)

[2 Progress 3](#_Toc464824180)

[3 Primary Objectives 3](#_Toc464824181)

[4 Scope 3](#_Toc464824182)

[5 Architecture 4](#_Toc464824183)

[6 Literature Review 5](#_Toc464824184)

[6.1 An Overview of Wi-Fi Direct 5](#_Toc464824185)

[6.2 An Overview of DSRC 5](#_Toc464824186)

[6.3 Performance comparison with DSRC 6](#_Toc464824187)

[6.4 Issues with Wi-Fi Direct 7](#_Toc464824188)

[7 Possible Improvements 7](#_Toc464824189)

[8 Alternative Strategies 8](#_Toc464824190)

[9 Benefits and Beneficiaries 9](#_Toc464824191)

[10 Risks 10](#_Toc464824192)

[10.1 Financial Risks 10](#_Toc464824193)

[10.2 Technical Risks 10](#_Toc464824194)

[11 Resource Requirements 10](#_Toc464824195)

[12 Budget and Funding 11](#_Toc464824196)

[13 Task Allocation 11](#_Toc464824197)

[14 Time Plan 11](#_Toc464824198)

# Problem Statement

Dedicated Short Range Communication (DSRC) carries lots of shortcomings in its implementation in Intelligent Transportation Systems (ITS); Hardware available only in newer vehicles, Hardware cost, likely to take a long time to deploy, Pedestrians cannot be included. Therefore it is necessary to come up with an alternative for DSRC.

# Progress

* Measured Wi-Fi Direct signal range
* Developed and tested an Android application for communication with Wi-Fi Direct. This requires manual authentication.
* Developed and tested an Android application that does not require user involvement in authentication phase.
* Monitored wireless traffic using Wireshark.
* Tested a Wi-Fi Direct open-source library on a rooted Android phone. Used Android terminal to run commands.

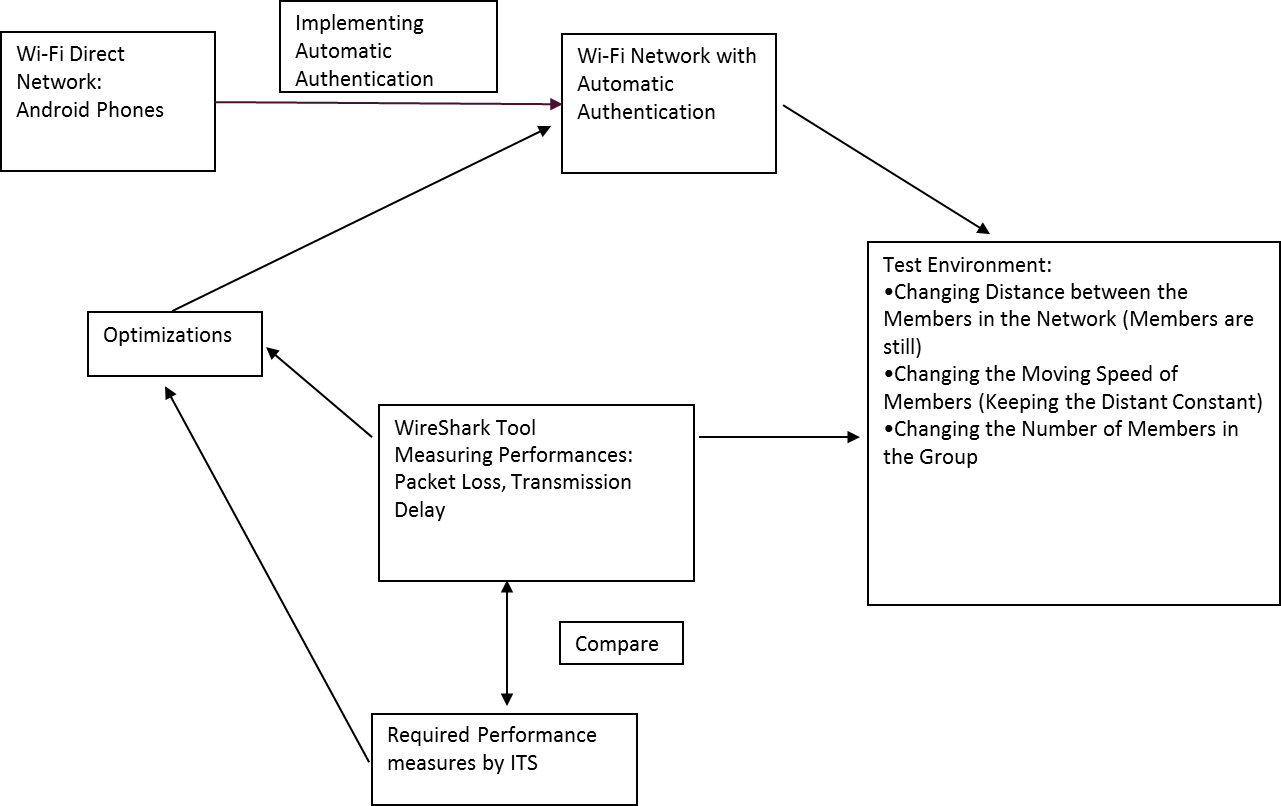
# Primary Objectives

1. Create a Wi-Fi direct network
2. Measure the performance of the network
3. Suggest and implement improvements for the network
4. Compare performance

# Scope

1. **Create a Wi-Fi Direct network using Android phones:** An Android phone represents a node in the network. The network uses Wi-Fi Direct as the communication protocol. Nodes should be able to dynamically create connections and maintain connections. In addition, nodes should be able to exchange data messages with each other.
2. **Implement automatic authentication feature in the Wi-Fi network:** Since it is not practical to have a user manually authenticate connections in a large network and manual authentication adds to the delay of connection establishment, automatic authentication feature should be available in network nodes. Since Wi-Fi Direct API for Android does not support automatic authentication, this feature should be implemented using different methods which are described in the literature review.
3. **Monitor network packets using Wireshark:** Use a laptop running Wireshark to monitor network traffic. Using this data, it is possible to calculate necessary performance measures.
4. **Measure performance:** Using the data gathered from Wireshark calculate the necessary performance measures (packet losses, transmission delays with respect to distance between members, speed and number of members in the group etc.)
5. **Compare measured performance with required performance:** Measured performance from the previous step will be compared with required performance for a vehicle to vehicle communication protocol (e.g.: compare measured message delays with the required message delay of 100ms). This process will help us to evaluate the suitability of Wi-Fi Direct for vehicle to vehicle communication system.
6. **Suggest and implement suitable improvements for the current network:** There are suggested improvements for the Wi-Fi Direct protocol, especially to minimize its delays, which are included in the literature review. These optimizations will be implemented in the network and we will repeat the process from step 3. Then we can evaluate the experimented effect of these optimizations.

# Architecture



# Literature Review

## An Overview of Wi-Fi Direct

Wi-Fi Direct was introduced in order to improve direct device to device communication using the bandwidth allocated for Wi-Fi (IEEE 802.11 standard). Wi-Fi supports data rates up to 2Mbps and operates in the 2.4 GHz bandwidth. Wi-Fi Direct is based on the IEEE 802.11n standard and it operates in the 5/2.4 GHz bandwidth. It supports data rates up to 250 Mbps and uses WPA2 and AES 256 bit encryption for security. The operating range for Wi-Fi Direct is up to 200m and it offers two-way area coverage. Further, it provides the opportunity for Wi-Fi Direct software to be installed in legacy Wi-Fi certified smartphones without any additional cost.

The special feature of Wi-Fi Direct is that it allows device-to-device connectivity in the absence of an Access Point (AP) which is used in traditional Wi-Fi networks. Wi-Fi Direct is built upon IEEE 802.11 infrastructure mode where a soft AP is created. Unlike the earlier technologies, Wi-Fi Direct allows devices to agree on a device to act as the AP. In typical Wi-Fi networks, an AP creates WLANs for clients to join. Here a device can behave either as an AP or as a client. However, Wi-Fi Direct allows a device to implement both roles. Since the roles are logical, they can be executed simultaneously either by using different frequencies or by using different time slots.

Wi-Fi Direct devices communicate with each other after forming P2P groups. For the formation of a P2P Group, it requires a minimum of one device that supports Wi-Fi Direct and the other devices can be legacy Wi-Fi Certified devices. In order to identify a group there is a name for the group which is known as the Service Set Identifier (SSID). It is the GO that provides the SSID and WPA2 authentication to the group members. Channels 1, 6 and 11 in 2.4GHz bandwidth are the operation channels available for a GO to select for a group. The Client devices need to have Wi-Fi Protected Setup (WPS) enrollee functionality, as it provides security within the group.

## An Overview of DSRC

Dedicated short-range communication (DSRC) is a popular technology for exchanging of safety and non-safety information between vehicles and between vehicles and infrastructure. IEEE 802.11p and IEEE P1609.x standards defines DSRC addressing transmission of safety information over a radio link in a vehicular environment. Data rates ranging from 3Mbps to 27Mbps can be achieved through DSRC. The Federal Communications Commission (FCC) allocated 75 MHz bandwidth to be used by the Intelligent Transport Systems for research and development of safety applications in vehicles.

DSRC equipment are required to implement the V2V or V2I communication in the real business. These devices work as transceivers where transmitting and receiving safety messages. The transceivers which are installed in vehicles are called On Board Units (OBU) which is capable of broadcasting Basic Safety Messages (BSM) such as vehicle location, speed, heading direction. The other type of unit is Road Side Units (RSU) which is installed in infrastructure like Street Signal posts or lamp posts etc. Each RSU has an individual communication zone (more like a coverage zone) called Wireless Access in Vehicular Environment Basic Service Set (WAVE BSS/ WBSS). At a given time, one vehicle is connected with only one WBSS. When the vehicle travels, it changes the WBSS which it belongs to.

DSRC is a promising technology; Latency, Speed, Bandwidth etc. are finely tuned with the expected requirements of safety message system in V2V environments. However, it contains a major drawback. It is that the DSRC equipment has to be installed in vehicles at an additional cost. Although the models to arrive can be expected to carry a DSRC unit, most of the existing vehicles do not carry it. Further this way is not going to bring the pedestrians into the communication network since pedestrians carrying DSRC equipment is not feasible in a practical sense. Therefore, now the trend is biased towards the use of Wi-Fi Direct for communication between vehicles-vehicles and pedestrians-vehicles because pedestrians carrying a Smartphone or tablet can be used for this purpose.

## Performance comparison with DSRC

DSRC operates on 5.9GHz band while Wi-Fi Direct operates on 5GHz or 2.4GHz bands [1]. DSRC has 10MHz of channel bandwidth and 6-27Mbps data rate [1]. Wi-Fi Direct has 20MHz of bandwidth and thus a higher date rate up to 250Mbps [1]. For encryption, DSRC uses elliptic curve cryptography with 256-bit keys and Wi-Fi Direct uses Advanced Encryption Standard (AES) 256-bit encryption [1]. DSRC has an operating range from 100m to 1000m while Wi-Fi Direct has only about 200m [1]. Although DSRC is tailor made for the use of communication in ITS, it has some shortcomings especially in practicality.

* **Hardware**: DSRC requires dedicated hardware. To add to the problem, DSRC hardware is very expensive at the moment (about $350 [1]), and this will definitely hinder the number of sales since these devices are highly price elastic. Wi-Fi Direct hardware, on the other hand, is very cheap and almost all new Android smart phones have it.
* **Pedestrians**: If we are to use DSRC for communications in ITS, then we will not be able to include pedestrians in our transportation systems, because pedestrians do not carry DSRC hardware with themselves. However, if we are to use Wi-Fi Direct instead, then we will be able to do this since the majority of the population (in most countries) carry smart phones.
* **Deployment**: Since DSRC hardware is expensive and only available in newer vehicles, it is fair to guess that it might take a long time to properly test and deploy in an ITS.

## Issues with Wi-Fi Direct

Wi-Fi Direct is a technology which is designed to exchange files or data between devices without the need for an Access Point unlike normal Wi-Fi. However, since group forming is not required to be very quick in normal device to device communication, group formation can take a long time to complete, like 20 seconds [3].

Another issue with Wi-Fi Direct is that it uses Wi-Fi Protected Setup (WPS) for authentication. This means that a user will have to be present at all times to authenticate a connection between another device. This becomes a critical problem in using Wi-Fi Direct for vehicular ad-hoc networks. However, this issue can be overcome by several methods, including rooting android phones, creating a soft-AP using Wi-Fi Direct and connecting to it as a legacy Wi-Fi client [2] etc.

In Wi-Fi Direct all messages go through the group owner. This means that if the message is intended for more than one group member, then group owner will have to transmit the same message more than once to different recipients. It has been theoretically proven that, the maximum number of vehicles for a group is 22 in order to fulfill the message delivery time requirement of 100ms [1].

# Possible Improvements

Here we are introducing the Soft Access point (Soft-AP) concept to solve the issue where one or more devices can connect simultaneously if they know AP’s SSID and pre-shared key. However, neither SSID nor pre-shared key of the soft access point cannot store beforehand since it generates and changes every time the soft AP is created [**2].** Therefore, with the use of Network Service Discovery (NSD) broadcast message we are able to pack both pre-shared key and SSID and send wirelessly from access point to all neighbor devices by Wi-Fi Direct framework. If one device is receiving more than one NSD message from AP it can act as a relay point and it can connect to any AP. Both pre-shared key and SSID are encrypted using AES-CCMP or TKI [**2]** and the key used for encryption is stored beforehand. In addition to single point to multipoint connection this method enables an automated authentication process which will affect in reducing the group formation delay. Broadcasting message has to be sent with universally unique identifier (UUID) and MAC address of its origin. If the message is repeated, following messages after first one may be discarded and ignored based on the stored UUIDs. If a new message is identified then process information, append the AP MAC address to the header and finally send it out.

Now we are looking at a new WD2 algorithm of selecting Wi-Fi Direct GO. In this scenario each device receives an Intent Value(IV) from every other node during the discovery phase and select the largest IV value device as GO while publishing it to all other nodes. Next it requires calculating the IV value correctly which eventually results in accurate RSSI value. In order to increase the accuracy, the number of probe packets has been increased and received node calculates its average RSSI value as well as each node keeps an average RSSI value list of discovered peers. Then based on the RSSI list values calculate the IV value of device ‘i’ as follows.



# Alternative Strategies

Following are possible alternatives we have identified. The advantages and drawbacks of choosing those methods are explained below.

* **Nodes**: Any one of Wi-Fi modules, laptops or Android phones can be selected as the nodes of the network. If Wi-Fi modules are selected, then they will have to be used with microcontroller. This presents us with many problems such as supplying power, dealing with unreliability, loose connections and coding in a very low level. In addition, many of Wi-Fi Direct modules does not support the full Wi-Fi Direct protocol, instead they only have the ability to behave as soft access points. Laptops should be used with Wi-Fi Direct libraries. Although open-source libraries exist for Wi-Fi Direct, this option is rejected due to the lesser mobility of laptops and hardware requirements. Compared to mobile phones laptops are less mobile. In addition, only newer laptops have hardware support for Wi-Fi Direct. In contrast, many Android phones have hardware support for Wi-Fi Direct and they are very inexpensive. Android provides very popular APIs to work with Wi-Fi Direct, so coding time is minimized and reliability is ensured.
* **Authentication:** As the authentication method we can use WPS which is already available in Wi-Fi Direct, WPA2 which is extensively used in Wi-Fi, or rooted Android phones with automatic authentication. WPS authentication requires a user to be present, so this is impractical for an ad-hoc network where connections are made and removed frequently. In addition, this introduces a delay in connection, which can affect performance calculations in later stages. WPA2 authentication enables automatic authentication, but it uses Wi-Fi, not Wi-Fi Direct. This restricts us from observing group formation and group owner negotiation delays which are critical delays with regard to assessing the suitability of Wi-Fi Direct for a vehicle to vehicle communication network. Rooting android phones would allow us to keep on using Wi-Fi Direct and it will enable automatic authentication.
* **Monitoring:** Wireshark or log files can be used for this task. Wireshark is a very popular network analyzer. It provides sufficient information to calculate the required performance measures. Collected data from Wireshark can be taken out in many different formats (e.g.: spreadsheets), so data processing is easy. Alternatively, log files can be used to log necessary information related to the network. This can include information which cannot be detected by a network monitoring tool. However, processing this data can be difficult.

Considering the reasons listed above our chosen strategy is to use Android phones as network nodes, root Android phones to enable automatic authentication and use both Wireshark and log files to monitor the network.

# Benefits and Beneficiaries

* ITS designers
* General Public
* 3rd World Communities (since DSRC penetration is very low and availability of Wi-Fi Direct)
* Research Community

# Risks

## Financial Risks:

Due to the inherent risk of rooting an Android phone, there is a risk that we might have to pay for a mobile phone that is damaged. However, in order to mitigate this risk, we are hoping to be very careful and responsible when rooting and working with rooted Android phones.

Another financial risk is having to buy Android phones for experimental purposes. This occurs only if we fail to find a provider for Android phones. In case this risk occurs, we could use our personal Android phones for experimental purposes. If the number of phones is not enough, it is possible to use the funding available for this project. Since used Android phones are available for an affordable price, we would be able to buy adequate number of Android phones for our experimentation.

## Technical Risks:

Android apps work differently in different Android versions. The apps that may find work reliably in one Android version, might not work at all in another one. This is especially relevant to Wi-Fi related applications, because the newer Android operating systems filters out Wi-Fi signals considering many facts. For example, newer Android versions (Lollipop or higher) doesn’t let the user accept poor Wi-Fi connections. Even the option to let the user select whether to accept poor connections is removed in newer versions. In order to overcome this issue, we are hoping to use phones with the same Android version. So, different processing steps in the Android framework wouldn’t affect our calculated delays. Hence our results would more accurately represent Wi-Fi Direct performance.

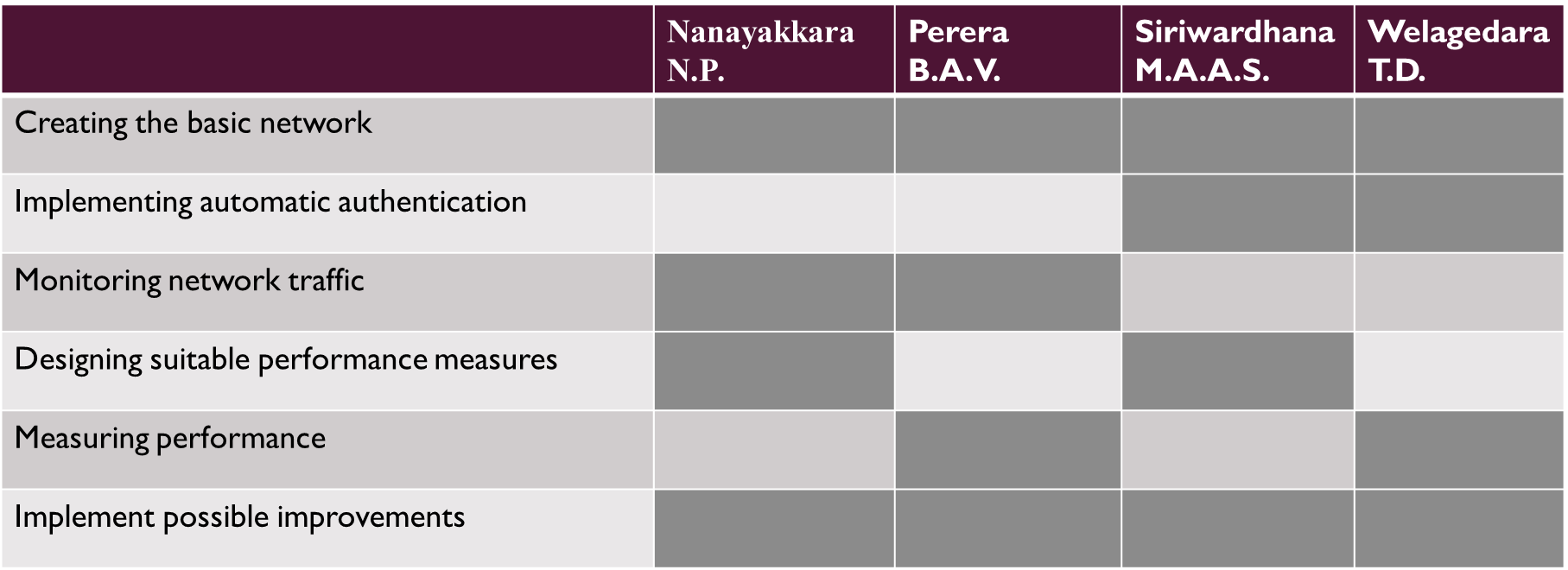
# Resource Requirements

* Android phones – At least 7 or preferably more Android phones are required. These phones needed to be rooted, so the provider should take that risk into account.
* Wi-Fi signal free area – Due to the ease of monitoring Wi-Fi traffic, it is desirable to use a wireless signal free area for experimentation.
* Vehicles – Vehicles will be needed to add mobility to network nodes. In face vehicles in public roads is the required communication environment where performance in Wi-Fi Direct needs to be tested.

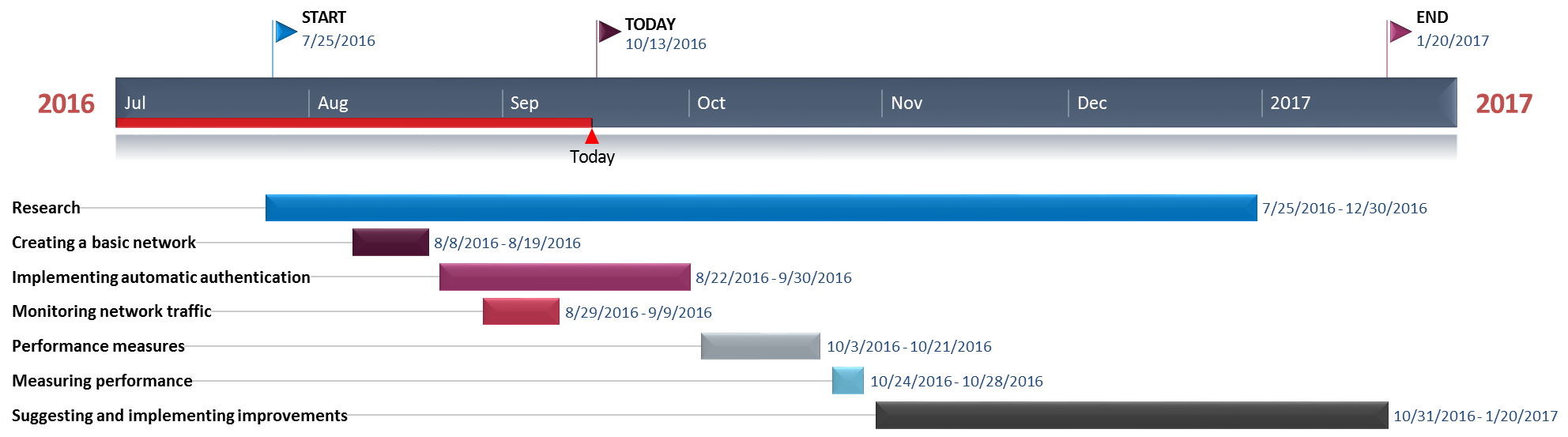
# Budget and Funding

If the available number of Android phones is enough, then no further funding is required.

# Task Allocation



# Time Plan



**References**

[1] Satish, Chaitra, "Inter-vehicular communication for collision avoidance using Wi-Fi Direct" (2014). Thesis. Rochester Institute of Technology. Accessed from  
http://scholarworks.rit.edu/theses/7664

[2] P. Wong, V. Varikota, D. Nguyen, A. Abukmail, “Automatic Android-based Wireless Mesh Networks.” Informatica (Slovenia), 38(4), 2014.

[3] D. Camps-Mur A. Garcia-Saavedra and P. Serrano "Device-to-device communications with Wi-Fi direct: Overview and experimentation" **IEEE Wireless Commun. Mag.** vol. 20 no. 3 pp. 96-104 Jun. 2012.