2016

An investigation of potential wireless security issues in traffic lights

Brian Bettany
School of Science, Security Research Institute, Edith Cowan University, bbettany@our.ecu.edu.au

Michael N. Johnstone
School of Science, Security Research Institute, Edith Cowan University, m.johnstone@ecu.edu.au

Matthew Peacock
School of Science, Security Research Institute,Edith Cowan University, mpeacock@our.ecu.edu.au

DOI: 10.4225/75/58a69541f370c
Bettany, B., Johnstone, M. N., & Peacock, M. (2016). An investigation of potential wireless security issues in traffic lights. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia*. (pp. 76-82).

AN INVESTIGATION OF POTENTIAL WIRELESS SECURITY ISSUES IN TRAFFIC LIGHTS

Brian Bettany[1], Michael N. Johnstone[1, 2], Matthew Peacock[1, 2]
[1]School of Science, [2]Security Research Institute
Edith Cowan University, Perth, Australia
bbettany@our.ecu.edu.au, m.johnstone@ecu.edu.au, m.peacock@ecu.edu.au

Abstract

The purpose of automated traffic light systems is to safely and effectively manage the flow of vehicles through (usually) urban environments. Through the use of wireless-based communication protocols, sets of traffic lights are increasingly being connected to larger systems and also being remotely accessed for management purposes, both for monitoring and emergency purposes. These protocols, however, were not designed with security as a primary requirement, thus systems may operate with sub-standard or non-existent security implementations. This research aims to test if the same issues and vulnerabilities that appear to be present in traffic light systems in the USA are prevalent in Australia, specifically, Perth. There is evidence of weaknesses in traffic systems in Eastern Australia and by undertaking this research the conjecture that the same weaknesses may be present in Perth traffic systems can be answered. While none of three common wireless protocols (ZigBee, Bluetooth or Wi-Fi) were found to be in-use, the discovery of a large, consistent network pulse warranted further investigation at one specific intersection.

Keywords
Wireless Protocol, Critical Infrastructure, Cyber Security

INTRODUCTION

Traffic lights have existed in some form for over a century, with the first coloured signal light system appearing in 1914 in London, England (Helmer, Meth, & Young, 2015), consisting of two semaphore arms lit by gas lights. Mueller (1970) notes that by 1915 parts of America were trialling a similar system except it incorporated electric lights and contained a small rotary compressor to blow a whistle, a method well-established at the time by on-duty policemen to control traffic. In 1920 the first three-light (Red, Amber and Green) system was installed in Detroit, Michigan and represents the beginning of what would be conventionally recognised as the modern traffic light.

These early lights are somewhat unsophisticated compared to the traffic lights in use today. Mladenovic (2012) states that traffic lights are now part of a much larger system that is controlled by a central computer using programs such as SCATS (Sydney Coordinated Adaptive Traffic System) or SCOOT (Split Cycle Offset Optimisation Technique). These systems can measure traffic volumes used in road sensors and adjust light timings to allow for the most efficient flow of traffic, not only in a single set of traffic lights, but throughout a whole city.

The motivation for efficient movement of traffic is simple: traffic jams cost time and therefore money. Hodson (2014) estimates that the combined economic loss from traffic congestion for France, the UK, Germany and the USA will increase from USD $200 billion in 2013 to $293 billion by 2030. The total economic losses equate to $4.4 trillion over this 17 year period. These figures represent both the direct (cost of fuel and time wasted) and indirect costs (increased cost of doing business) caused by traffic congestion. The study predicts that the average hours wasted in traffic will increase by 6% by 2030. It also highlighted the environmental cost of this congestion, suggesting that in the four countries studied, idling vehicles released 15,434 kilotons of CO_2 into the atmosphere and that this figure will increase to 17,959 kilotons by 2030. Therefore, any attack (cyber-based or otherwise) on systems that control traffic need only be moderately successful to have a large impact on the economic well-being of a country.

Traffic systems are a vital part of the critical infrastructure of any city, and a city's economic and social well-being is dependent on the smooth movement of people and freight. It could therefore be assumed that any disruption to this system will have some form of impact. This does not have to be a major disruption to have a

potentially devastating effect, for example consider emergency vehicles not being able to get to where they have to be because they are caught in a traffic jam caused by a traffic system failure (Kelly, 2001).

Cerrudo (2014) claims to able to hack into the traffic lights in several United States cities, including Washington DC and New York City, and potentially alter the timings of the signals. Cerrudo (2014) showed how to intercept the wireless signals that were being transmitted from a sensor node in the roadway to a traffic controller located on the road-side using commercial off the shelf tools. The specific system in question is produced and marketed by Sensys Networks which, according to their sales literature, is used extensively around the world including Australia (Ford, 2015).

This research aims to test if the same identified issues and vulnerabilities that appear to be present in traffic light systems in the USA are prevalent in Australia, specifically, in the city of Perth. The remainder of the paper describes some specific instances of traffic or traffic-related attacks, defines the experimental methodology used and discusses the findings of the research.

SECURITY ISSUES IN TRAFFIC LIGHT SYSTEMS

Much like the advancement of other service-based systems, traffic lights were not designed with security as a principal requirement. Early security of these systems revolved around physical isolation and proprietary protocols. However, with increased connectivity for remote management and operation, and the use of common protocols for interoperability, the security through obscurity paradigm no longer applies to these critical systems.

There is limited peer-reviewed research on the security of traffic lights. Estrin (2013) reports that in September 2013 cyber-terrorists attacked the traffic system in the Israeli city of Haifa, targeting the security camera network on the Carmel Tunnels toll road with what was believed to be a Trojan malware programme. The attack was carried out sporadically over two days, resulting in the roadway being shut down during the peak hour period, and remaining shut for a period of eight hours on the second day. The resulting traffic jam not only caused long delays to the commuters caught in it, but could have other less visible flow-on effects. These include the cost of any type of traffic congestion to business and risk to life should emergency vehicles be stopped or delayed by the traffic jam (Bernasek, 2014; Kelly, 2001, Schrank, Eisele, & Lomax, 2012). While this attack was an extreme case, with driverless cars currently in the trial phase, security issues in traffic light systems are a risk that will need to be managed, given the increased automated interaction between driverless cars and traffic light systems (Petit & Shladover, 2014). There has been limited research into the vulnerabilities of these systems carried out in the USA (Cerrudo, 2014; Ghena, et al., 2014), with very little consideration of whether these same vulnerabilities are present in systems used in Australia.

A team from the University of Michigan (Ghena et al., 2014) investigated local traffic light systems. In the Michigan area, traffic light systems use induction loops below the ground to detect cars, which then communicate using wireless signals between the traffic controllers and the central server. The central server is capable of making modifications to the light timings dependent on the information it receives from the induction loop sensors, to dynamically avoid or alleviate traffic congestion. Each traffic intersection is treated as an individual isolated system, with communication and coordination between intersections undertaken using a central server. The protocol used for these wireless communications is a proprietary protocol similar to 802.11 Wi-Fi; which presents an SSID visible from a normal laptop or smartphone.

With the cooperation of a road agency in Michigan, Ghena et al (2014) went on to show that it was possible to compromise traffic lights in Michigan by using the communication radio signals used by the network. These fell into two ranges, 5.8GHz for short distance in-line signals and 900MHz for longer distances blocked by buildings or other obstacles. They found three major problems with these traffic communications:

1. Wireless signals were not encrypted
2. Default usernames and passwords were used
3. Known exploits could be used

These weaknesses allowed for attacks such as Denial of Service (DoS), timing manipulations to cause congestion and the ability to exploit these weaknesses while driving to ensure a green light wherever you go.

It was shown that at least in these types of traffic controllers the more extreme claims of deaths or accidents resulting from all the lights turning green are highly unlikely unless physical access to the traffic control box can be achieved, because a hardware system is in place which stops this event happening.

Government Audits

Similar to the US, there is little publicly-available information about the security of traffic systems in Australia. There have, however, been two Australian State Governments that have run audits on their traffic systems in the past five years, with both identifying a number of weaknesses (Gaskell et al., 2015; QUA, 2013).

The Queensland Government audit undertaken before the 2014 G20 conference in Brisbane identified a lack of security understanding, and a wide range of security issues. The report states, "The traffic management systems for the Brisbane metropolitan area were not secure. If the systems were specifically targeted, hackers could access the system and potentially cause traffic congestion, public inconvenience and affect emergency response times. Such attacks could also cause appreciable economic consequences in terms of lost productivity. It was identified that these issues were caused due to increased connectivity between control systems and the Internet for remote management purposes" (QUA, 2013). A similar audit, released by the Audit Office of New South Wales in 2015 also found significant security issues in the traffic management system, stating that the risk management process put in place had covered the Transport Management Centre infrastructure, but the scope did not include the traffic network. Of note was one particular section of the road network, which had an identified lack of security and could lead to traffic disruptions, avoidable accidents or even the loss of life (Gaskell et al., 2015). These audits did not disclose specific details of the vulnerabilities discovered, but it is clear from the findings that there were concerns as to the security of the traffic system at a holistic level. In response to these audits the relevant government departments of both states have stated that they have made, or are making the necessary changes to the systems, security practices and security education and awareness training for staff. At this time there is no evidence the WA government has audited the traffic control systems in Perth, in relation to their susceptibility to cyber-attack. The aim of this research is thus to investigate if wireless security issues of traffic sensors, identified in the US, and in operation in Eastern Australia, are in use and/or prevalent in Perth.

RESEARCH METHOD

The research was designed as a number of field experiments, where a combination of appropriate hardware and software resources were used to try and detect, capture and then analyse specific wireless communication used by a selection of traffic lights in Perth. Each step (hypothesis, defined in Table 1) is dependent on its precursor.

The initial focus of this research was to ascertain if the same wireless security issues described by Cerrudo (2014) were present in traffic systems used in Perth. There was evidence that these systems are in use in Melbourne ("M80 FWY Management System", 2012; "Sensys networks freeway solutions, Melbourne", 2010), so there was a possibility that they could also be in use here in Perth.

To answer the key research question, viz. *"Could the same security concerns highlighted in America in regard to ZigBee be present in the traffic systems here in Perth?"*, a number of hypotheses were proposed and are presented in Table 1.

The research was focused on the way traffic light systems communicate at the intersection level and whether specific wireless communications, namely ZigBee, are used. ZigBee was selected because, whilst Cerrudo, (2014) did not specify the protocol he examined, it is clear from the evidence he presented that he protocol was ZigBee. The field experiments to examine these communications were undertaken between March and June 2016 at multiple traffic intersections in Perth. These intersections were chosen because they allowed easy and safe access and represented a cross section of the traffic lights in the eastern and western suburbs of Perth.

Table 1: Hypotheses to be tested

Hypotheses
H_1: ZigBee can be detected in use for wireless communication by traffic lights in Perth.
H_2: The ZigBee packets used by the traffic lights can be captured for analysis.
H_3: The ZigBee traffic used by the traffic lights is encrypted.
H_4: Default settings for authentication are being used by ZigBee traffic systems.
H_5: ZigBee traffic is susceptible to attack with the KillerBee framework.
H_6: New nodes can connect to the traffic system using zbassocflood to a point where the system overloads.
H_7: Legitimate commands can be sent to the traffic system using zbreplay and accepted.
H_8: Legitimate commands are accepted and can be used to change the timings of the traffic lights.

Materials

The initial aim of capturing transmitted packets involved passively sniffing at the traffic intersection; to do this the following equipment was used:

1. HP Laptop (Pavillion dv6) with Windows 8.1 (64 bit) operating system
2. VMware Workstation 12 Player virtual machine running Kali-linux-2016.1-amd64
3. Wireshark version 2.0.1 installed as part of Kali-linux-2016.1-amd64
4. Atmel RZUSBstick antenna configured to work with the ZigBee protocol
5. KillerBee 1.0 Framework running on Kali-linux-2016.1-amd64

ANALYSIS AND DISCUSSION

According to Main Roads WA, Perth has over 850 sets of traffic lights in use throughout the metropolitan area ("Traffic Signals", 2015). These traffic lights are controlled using SCATS and a typical layout for the overall system is shown in Figure 1, whilst Figure 2 shows a typical intersection layout.

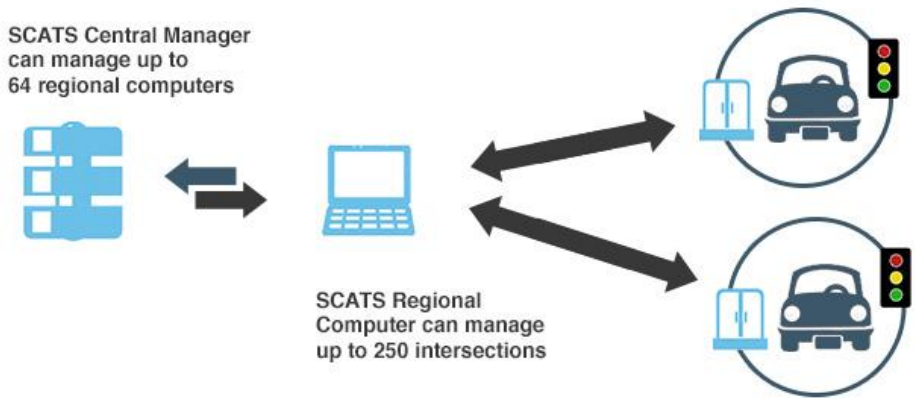

Figure 1: SCATS Control Hierarchy Layout.

The intersections examined consisted of a series of in-road sensors (induction loops) that are connected to a road side control box, which is subsequently connected to both the traffic lights and the regional control centre.

A car moving down the road is picked up by the in-road sensor, which sends this information to the roadside control box. The information is then sent back to the regional computer that performs an analysis, consisting of all the information provided by the other intersections in the area that it controls. The stated configuration gives the regional controller an overview of traffic conditions in a wide area, allowing intelligent decisions to be made to adjust traffic light times accordingly. The most appropriate timings are then sent back to the roadside controller, which then implements the timings through control of the associated traffic lights (Dineen & Cahill, 2001). A central control centre manages the regional controllers, allowing oversight and manual manipulation of the system when necessary, such as in emergencies.

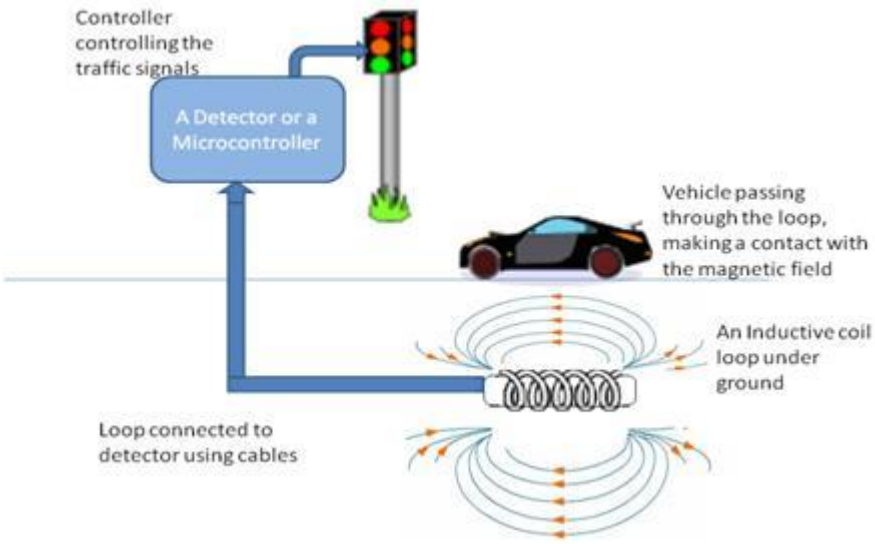

Figure 2: Typical Traffic Light Road layout, retrieved from Agarwal (2013)

Captures of the ZigBee protocol were attempted at ten different intersections in Perth, these tests being attempted on two separate occasions at each intersection and when possible, on different days and times. No traffic was detected on any channel, thus disproving H_1 and effectively invalidating the remaining hypotheses defined in Table 1. This result led to a re-focusing and re-evaluation of the research goal whereby other common wireless protocols were examined. The research question was re-framed as:

"*Is there any evidence that other wireless communication protocols are being used to transmit data between the components that make up an intersection set of traffic lights in Perth, specifically:*

a. Is Bluetooth (IEEE 802.15.1) used in the majority of traffic lights in Perth?

b. Is Wi-Fi (IEEE 802.11) used in the majority of traffic lights in Perth?"

Additional appropriate hypotheses were developed accordingly, to test the revised research question.

In addition to the materials described in the previous section, extra hardware (an Ubertooth One antenna 2015-10-R1) and software (Spectools -2015-10-R1) were utilised to enable detection and capture of these identified protocols.

Testing was undertaken at the same intersections as the ZigBee testing. A Spectools scan using the Ubertooth One was run at each intersection- a typical example being shown in Figure . The green line represents Bluetooth transmissions while the white lines are Wi-Fi.

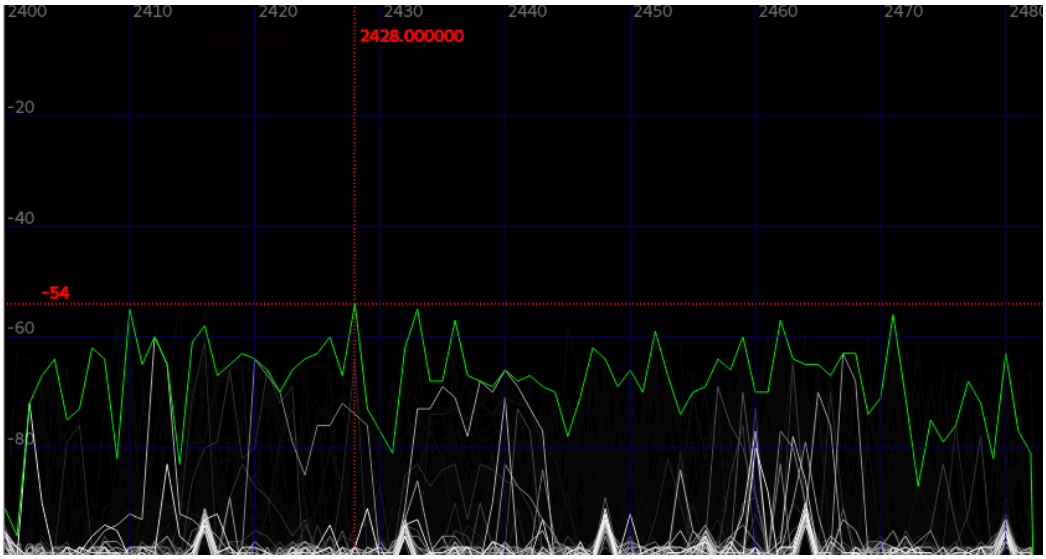

Figure 3: Ubertooth spectral analysis, depicting Wi-Fi and Bluetooth Activity

The Ubertooth One proved to be a useful spectrum analysis tool. It detected both protocols in the 2.4GHz range and displayed the traffic effectively. Although there were many transient devices at each intersection that were using Bluetooth (representing in-car systems and mobile phones used by pedestrians), there were no identified stationary Bluetooth devices at the traffic intersections (as the Bluetooth traffic did not have a static underlying pattern) based on the variable BD_ADDR identifiers detected during analysis.

Similarly, the Wi-Fi signals found were identified as nearby houses or businesses from their SSIDs and signal strength. There was no evidence to suggest that the 802.11 protocol was being used by the traffic lights to communicate to either another intersection or the roadside control box.

However, of note was a consistently identified network traffic pulse at one specific intersection. Upon further inspection of the surrounding traffic management infrastructure, a large antenna attached to the traffic light was identified as the source of the pulse. Spectral analysis was conducted on the pulse, but similar to other intersections, the pulse could not be classified as one of the investigated protocols, (ZigBee, Bluetooth or Wi-Fi), and thus was not captured or classified. The pulse occurred regularly at one-minute intervals, and was identifiable on two separate visits to the intersection, at similar times of day/days of week and peak traffic conditions. A third visit to the intersection resulted in no pulse being identified. While circumstantial, it should be noted that traffic conditions were much lighter during the third visit, which was conducted at a different time of day/day of week, compared to the previous two visits.

CONCLUSION

This research set out to look for the security flaws highlighted by Cerrudo (2014), in a traffic system that used in-road sensors connected via a wireless signal, namely ZigBee. As was outlined previously, there is some evidence that these systems are in use in Melbourne, but no such evidence was found in regard to the intersections investigated in Perth. The fact that there was no information on whether these systems were in service in Perth needed to be examined. The tools necessary for this examination were procured and testing was undertaken, however it became apparent that this protocol was not in use at the intersections tested. This result is a good outcome from a security viewpoint, considering traffic lights in Perth; if ZigBee is not being used it means it cannot be attacked via the methods outlined in Cerrudo (2014). This meant that the research project needed to be re-evaluated and modified to test a wider array of wireless protocols. Bluetooth and Wi-Fi were tested at the same intersections, using appropriate spectral analysis hardware and software. Similarly, there was no evidence of either Bluetooth or Wi-Fi being used by the traffic lights.

Finally, the discovery of a large, consistent network pulse warranted further investigation to one specific intersection. Further examination using the spectral analyser showed that none of the common wireless protocols (ZigBee, Bluetooth or Wi-Fi) were in use, similar to in other intersections investigated. Whilst purely circumstantial, the change in traffic conditions and related change in signal emission does add some weight to the argument that the identified pulse signal is being used by the traffic lights to transmit information during peak traffic periods. This is clearly an avenue for further research.

REFERENCES

Agarwal, T. (2013). Dynamic road traffic signal control system. Retrieved from https://www.elprocus.com/dynamic-road-traffic-signal-control/

Bernasek, A. (2014). The cost of getting stuck in traffic. *Newsweek*, 163.

Cerrudo, C. (2014). Hacking traffic control systems (U.S, UK, Australia, France, etc.). *DEF CON 22*, Las Vegas. Retrieved from https://www.youtube.com/watch?v=_j9lELCSZQw

Dineen, M., & Cahill, V. (2001). Towards an open architecture for Real-time Traffic Information Management. *Proceedings of the 8th World Congress on Intelligent Transport Systems*. Sydney, Australia

Estrin, D. (2013). Experts: Israeli tunnel hit by cyber attack. *Telegraph – Herald.* Retrieved from http://search.proquest.com/docview/144604498?

Ford, S. (2015). Audit project to evaluate vulnerability of traffic lights to cyber attacks. Retrieved from http://wjla.com/news/local/audit-project-to-evaluate-vulnerability-of-traffic-lights-to-cyber-attacks-114819#ixzz3dJSbTm2c

Gaskell, G., Avery, N., Crumlin, S., & Lo, K. (2015). New South Wales Auditor-General's report performance audit security of critical IT infrastructure. Retrieved from . https://www.audit.nsw.gov.au/ArticleDocuments/354/01_Security_of_Critical_IT_Infrastructure_Full_Report.pdf.aspx?Embed=Y

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, A. (2014). Green Lights Forever: Analyzing the Security of Traffic Infrastructure. *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14)*. Retrieved from https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Helmer, J., Meth, G., & Young, S. (2015). Sustainable traffic signal development. *ITE Journal*, 85(5), 14-19.

Hodson, H. (2014). Gridlock alert. *New Scientist, 223*(2981), 20. doi: http://dx.doi.org/10.1016/S0262-4079(14)61532-3

Kelly, D. (2001 Mar 12). Traffic jam + ambulance = total chaos. *Austin American Statesman*, p. B1. Retrieved from http://kx7gx4pm8t.search.serialssolutions.com/

M80 FWY Management System. (2012). Vicroads.

Mladenovic, M. (2012). Large scale analysis of traffic control systems. *Traffic Engineering & Control*, 53, 26+

Mueller, E. A. (1970). Aspects of the history of traffic signals. *IEEE Transactions on Vehicular Technology*, 19(1), 6-17. doi: 10.1109/T-VT.1970.23426

Petit, J., & Shladover, S. E. (2014). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2), 546-556. doi: 10.1109/TITS.2014.2342271

QUA. Traffic management systems: Report to parliament 5: 2013-2014. Technical report, Queensland Audit Office, 2013.

Schrank, D., Eisele, B., & Lomax, T. (2012). TTI's 2012 urban mobility report. *Texas A&M Transportation Institute. The Texas A&M University System,*

Sensys Networks Freeway Solutions, Melbourne. (2010). Youtube: Sensys Networks.

Traffic Signals. (2015). Retrieved from https://www.mainroads.wa.gov.au/UsingRoads/RoadTrafficInformation/Pages/trafficsignals.aspx