Australasian Transport Research Forum 2022 Proceedings
28-30 September, Adelaide, Australia
Publication website: http://www.atrf.info

Implementation of ZigBee-based WSN to enhance the performance of SCATS compatible intelligent traffic controllers

Hossein Parineh[1], Majid Sarvi[1], Saeed Asadi Bagloee[1]

[1]Department of Infrastructure Engineering

University of Melbourne

Melbourne, Australia

Email for correspondence: hparineh@student.unimelb.edu.au

Abstract

This paper presents a novel method for the interconnection of intelligent traffic control equipment at intersections. The practical method of linking the traffic control equipment at an intersection is wired, which has various drawbacks. By replacing the wired connection with the new wireless technologies, it is expected to not only increase the speed but also decrease the expenditures for the installation and maintenance of traffic control equipment at intersections. Moreover, the wireless method eliminates the common causes of failure in Intelligent Traffic Controllers (ITC), which is the main reason for losing coordination between intersections in a network. Thus, it helps keep the network nodes operable and maintain their KPI. To the best of our knowledge, this is the world's first application of Zigbee WSN for providing an intelligent and secure connection between Traffic Signal Heads (TSH) and ITCs that are SCATS compatible. Considering the required operational standards of ITCs, we designed two different electronic circuits controlled by ATMEGA64 microcontroller at both transmitter and receiver ends. For wireless communication, we selected ZigBee technology as a secure, low-cost, and low-power connection medium. ZigBee is an IEEE 802.15.4-based standard used for short and mid-range wireless communication. The device was designed, manufactured, and tested to provide the connection between the PSC-MK3 intelligent traffic controller to three individual receivers. Each receiver included two vehicle groups and two pedestrian groups. The performance of this solution was evaluated for more than three months and it proved to be stable and safe.

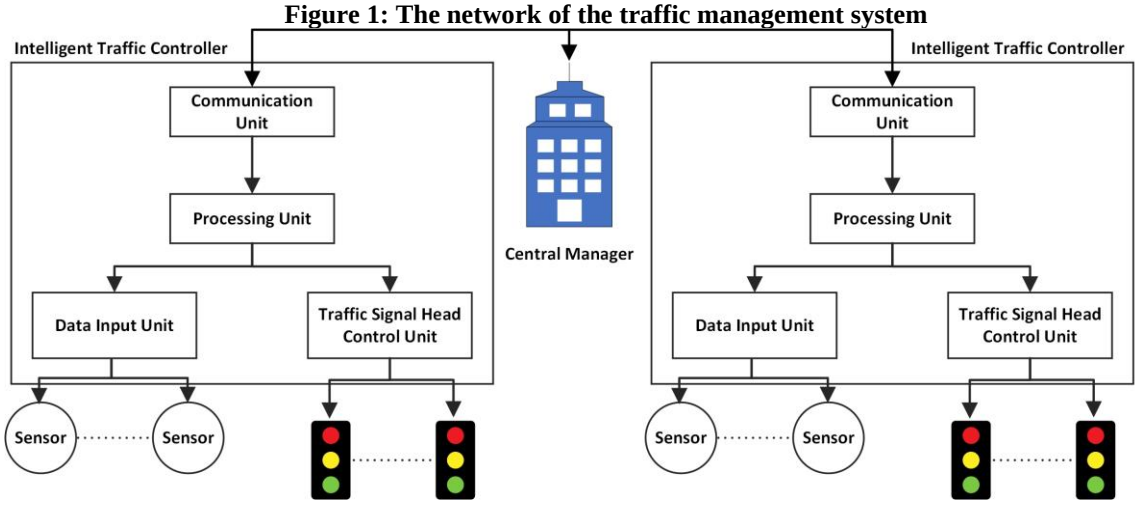
1. Introduction

The Intelligent transportation system (ITS) is an advanced technology that encompasses different fields of science (Qi, 2008). It integrates electronics, computer science, and communication and employs different types of sensors to not only increase safety for both vehicles and pedestrians but also enhance travel time, the efficiency of infrastructure use, and productivity, and reduce emissions (Zandi, 2011). The primary aim of ITS is to provide better applications of roads for commuters (Zhang, 2011). Regarding the importance of ITS for the sustainable development of cities, there is a considerable market for an efficient ITS solution. Based on a report, while the global market of ITS was about US$ 23 billion in 2018, it is estimated to reach over US$ 34 Billion by the year 2025 (Bhutani, 2019).

The Intelligent Traffic Controller (ITC) consists of two sections, the hardware, and the software. While the global trend of current research in this field focuses on the development of new software methodologies, there has not been significant research on hardware improvements. As shown in figure 1, the traffic control network consists of different types of sensors such as inductive loop detectors, Radar, LiDar, and cameras to gather information about the environment for the ITC. Then ITC either locally processes this data or transfers it to the central manager for updating the traffic management policy. Finally, the Traffic Signal Head (TSH) is controlled by the output unit of ITC. Conventionally, multicore cables are used for connecting ITC to TSH. This type of connection has several disadvantages in terms of time and expenditure of installation and maintenance, and the faults in ITC hardware that stem from cables. To illustrate, using cables requires expensive and timely civil work which is usually accompanied by closing the roads and aggravating traffic flow. Also, passing heavy vehicles over vulnerable cables or the presence of rodents in some countries could result in link disconnection between ITC and TSH. Also, in some countries, the TSHs are either not fully compatible with the input impedance of ITC or due to inaccurate electrical design, they produce reactive power that causes damage to output boards of ITCs, resulting in burnout in electronic parts of ITC (Department of Traffic and Marine Roads, 2015).

Regarding necessary safety standards considered for traffic control devices, any of the mentioned issues causes ITC to switch to flashing mode, leading to coordination loss between adjacent intersections and deteriorating the KPI of the whole traffic control network. Thus, finding a secure and stable wireless replacement for a wired connection is necessary. The notion of Zigbee was first introduced in 1998 and then regulated in 2003 as a global standard to provide the low-power wireless link for PAN (personal area networks) based on IEEE 802.15.4 standard. It is a low data-rate wireless personal network (LR-WAN) and is designed to operate with low power consumption and provide flexible network topology. This protocol is adapted and modified by different producers and they have added advanced complementary protocols in their personalized modules. ZigBee is used in occasions where we prefer real-time operation over bandwidth. The main reasons that ZigBee provides outstanding performance compared to other wireless technologies such as WiFi and Bluetooth are safety, power consumption, flexibility, and price (Danbatta, 2019) (Kumar, 2017). Compared to WiFi, Bluetooth, and other cheap wireless modules, ZigBee provides several additional features such as: “Medium Access Control” for managing the sequence of communications, “Addressing” to distinguish and access each module individually, and “Error Checking” which detects different types of errors such as single bit and burst errors, and “Encapsulation” that organizes diverse types of information in a single data packet.

Figure 1: The network of the traffic management system



2. Literature review

As mentioned before, regarding the complexity of design and essential SCATS standards to be followed, to the best of our knowledge this is the first application of ZigBee-based-WSN for the interconnection of traffic signal heads to the intelligent traffic controller. Thus, there is no similar work, and this literature review is focused on the definition of WSN and relevant applications of ZigBee in the field of traffic management.

A WSN consists of a few to thousands of mobile or static nodes working together to monitor and acquire data about the environment (Yick, 2008). WSN networks are categorized into two groups: tracking and monitoring (Zhang, 2012). In the field of traffic management, a conventional WSN includes sections for i) information collection, ii) data diffusion, iii) data processing, IV) decision making, and V) applying the new policy to the environment (Nellore, 2016). The WSN proposed in this paper focuses on sections i, ii, and V. Sections iii and IV are performed either by the intelligent traffic controller or the central manager of SCATS. Considering the facilities embedded in ZigBee protocol it has been employed for different tasks in traffic management systems. To tackle the problem of short-range communication in these devices the integration of ZigBee with the internet was considered in some research. To illustrate, a combination of internet and short-range wireless communication called SIP/ZigBee was used to connect adjacent intersections in a network (Zhou, 2011).

Transferring count values of road vehicle counters to real-time traffic monitoring, monitoring available parking lots, air quality, and natural disaster monitoring (flood detection) are part of the urban applications of WSN (Kandaris, 2020). Three major categories of employing WSN in the field of transportation are: i) Smart Cities such as pollution monitoring, ii) Traffic Management, for instance, parking management and linking intersections and vehicles to each other, and iii) Safety, like alarming other drivers in case of a vehicle violating red light or over-speeding (Kafi, 2013).

3. Proposed Model

There are diverse challenges in replacing the wired connection method with wireless technology. The first challenge is to understand the concept of operation in SCATS compatible ITCs and comply with the RTA (Road and Traffic Authority of NSW) standards. The next step is selecting a suitable network topology for ZigBee and designing the communication and security protocols based on it. And finally, these considerations must be applied within one or multiple well-designed microcontroller-based electronic circuits. This step also includes algorithm design and code development for microcontrollers. The code must also cover necessary security considerations for the network. To comply with the required standards of SCATS compatible ITCs, the device must follow certain rules. These rules are categorized into two groups, the concept of operation and the electrical specifications. To illustrate, for the first group, the ITC continuously monitors the lamp health status and in case of occurring a fault for a red lamp of vehicle signal groups, it will switch to flashing yellow mode to keep the safety for drivers. So, there must be continuous feedback from the traffic signal heads and applying it to ITC, to ensure safe operation at the intersection. For the second group, the input load for the ITC should be designed accurately to adapt the minimum watt and correct input impedance.

3.1. Operation Concepts and Design

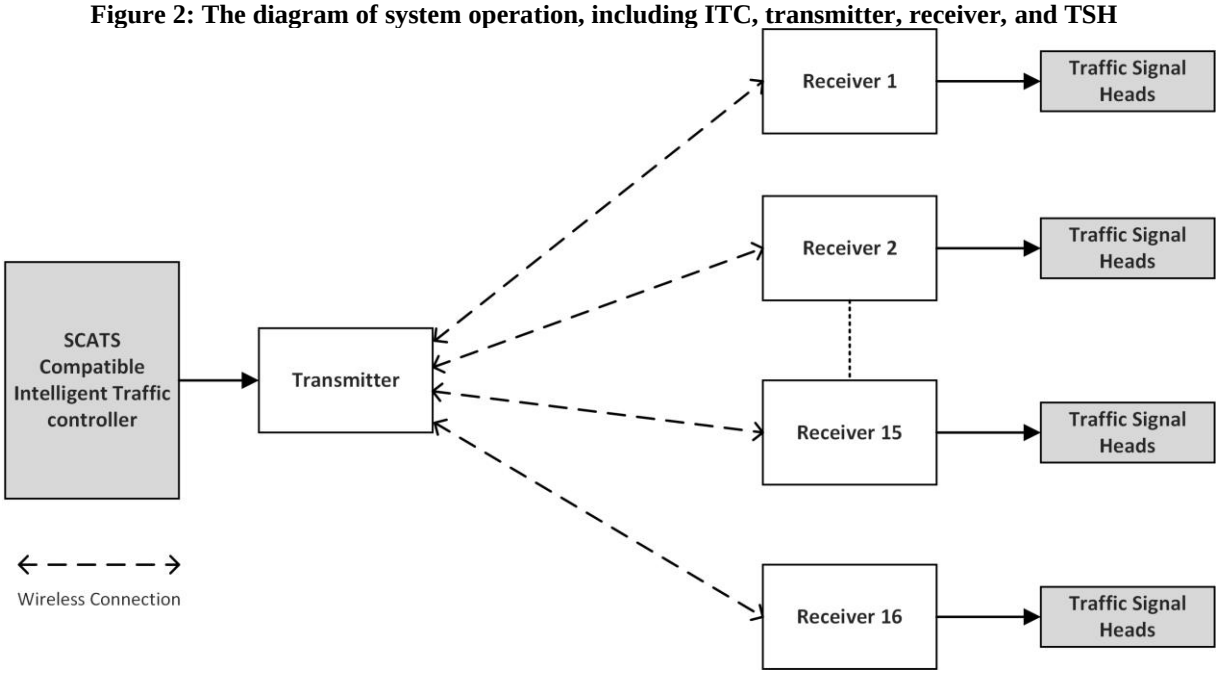
The overall structure for the system is shown in figure 2. it consists of two separate circuits as transmitter and receiver at ITC and TSH sides, respectively. At each intersection, only one transmitter is required to connect to the ITC. Transmitter has a section to read the momentary status of signal groups at the output of ITC, Then it encodes and encapsulates this data with additional information about the network it is managing and transmits the data to the receivers.

The transmitter can accept up to 16 independent receivers. Each receiver module can drive up to 6 different signal groups. The operator can assign any signal group to each available output.

3.2. Transmitter

The concept of operation for the transmitter is shown in figure 3. It includes two parts, the Sampling section, and the Transmitter section. The sampling section could consist of up to four boards, each board capable of reading data from four signal groups. To bring efficiency and

Figure 2: The diagram of system operation, including ITC, transmitter, receiver, and TSH



redundancy for the sampling section, instead of designing a monolith board with 16 signal groups, it was divided into four boards with 4 signal group inputs. Then, these sampling boards translate voltages from 230V into 5V DC, utilizable for the logic input of the transmitter circuit. The Transmitter receives this information and after ensuring the accuracy of the whole wireless network transmits the encoded and updated traffic signal status to the receivers.

3.3. Receiver

The scheme of the receiver is shown in figure 4. The receiver knowing the decipher key and the Private Area Network (PAN) that it belongs to, after receiving data from the transmitter, turns on/off relevant TSHs that it is responsible to control. In case of any failure in the TSH red lamps of vehicle groups, it informs the ITC so that the required actions could be taken. The TSH could be either vehicle (with three colors Red/Amber/Green) or pedestrian (with two colors Red/Green) signal groups.

3.4. ZigBee Module: XBee 3.0

XBee 3.0 is the latest generation of Digi wireless modules based on the ZigBee protocol (Digi website, 2022). It operates in ISM bands that include 915 MHz in Australia and the USA with 10 channels, 868 MHz in Europe with 1 channel, and 2.4 GHz in the rest of the world with 16 channels. The possibility to switch between accessible channels enables finding suitable channels with lower power and thus increases the stability of the network started in this channel. The nominal RF data rate is 250 Kbps and the outdoor range varies between 60m to 3200m which is achievable using different versions of this module. To provide security for the network, it has embedded 128/256 bit AES encryption. The memory of this module is

1MB/128KB RAM with a dedicated 32KB for MicroPython to directly code the device. While the supply voltage ranges from 2.1 to 3.6, the TX current for the maximum output power (8dBm) is only 40 mA and the receiving current is 17 mA. In power-down mode, the input current decreases to only 2 micro Amp at 25 degrees C.

Figure 3: The transmitter section, including sampling boards, the mainboard, and the radio board

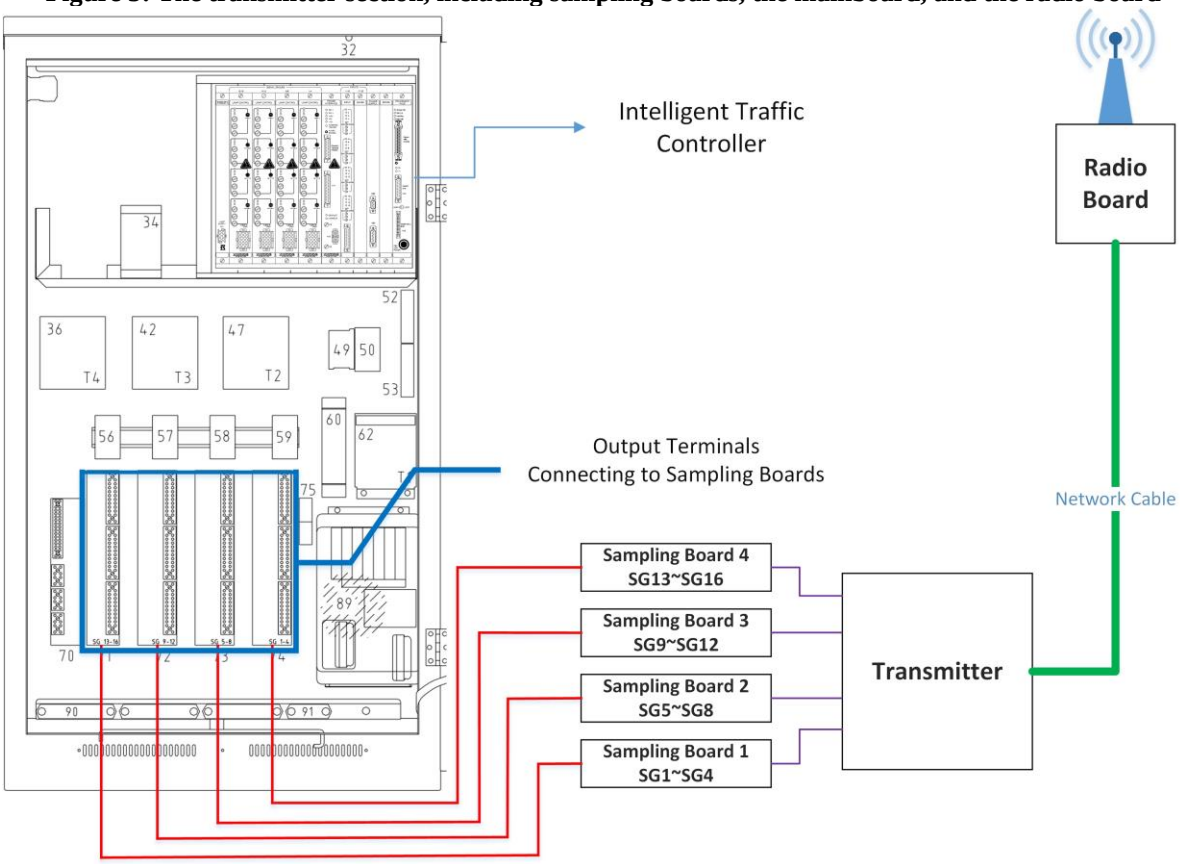
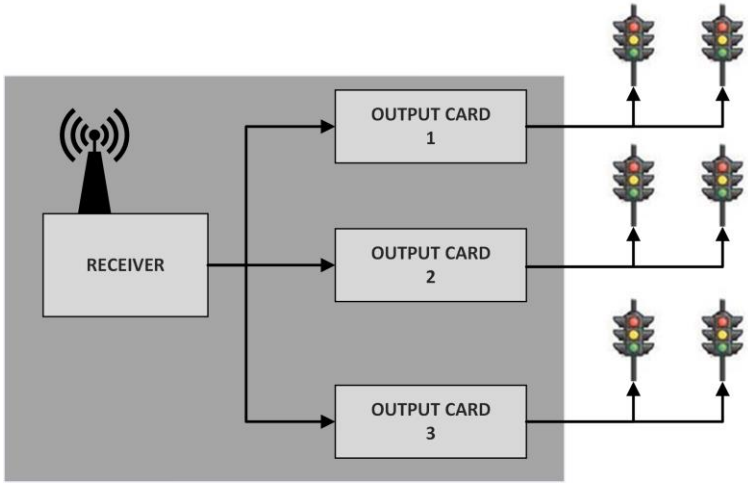


Figure 4: The receiver board, including the mainboard and transducer boards



3.5. Microcontroller: ATMEL ATMEGA64

The microcontroller works like a small computer on a single chip, responsible for different tasks at different levels of the system. These tasks include setting up the ZigBee network with

the suitable topology, ensuring the availability and functionality of all of the receivers, reading the next status of traffic signals from ITC, coding this data, transmitting it to the receivers, and making sure that they have received the data. To fulfill these tasks, the microcontroller used in this project is ATMEGA64. It is a 16MHz microcontroller with 53 I/O pins and two 8-bit timers that are used to keep the timings of the network. Thanks to the embedded ADC (analog-digital converter) unit, some environmental features such as light, humidity, and temperature could be measured with it.

3.6. Security

Regarding the importance of safety and security in traffic management systems, keeping data transmission secure against either intrusion, reply, interference, or jamming attack is an important concern. XBee benefits from a dedicated security policy devised by Digi called "TrustFence" which includes different levels of protection such as 128-bit AES encryption. This encryption is applied at both the network level and application layer (Digi website, 2022). Regarding the importance of security in wireless networks, different facilities have been embedded in the ZigBee-based modules. For instance, to protect the network against reply attacks, a 32-bit frame counter is used.

Also, Message Authentication Code (MAC) with 4 bytes hash code is appended to the network header, application header, and application data. Also, it is possible to decode and encode the messages in each node, however, it leads to latency in the network. For the application layer security, there are several features such as 4-bytes for Message Integrity Code (MIC), and application link key by the Trust Center Link Key.

A reply attack happens when a sniffer captures data packets and saves them, then resends the packet to mislead the receiver. It happens when ZigBee encryption or trust center is not active, or for the mac layer of 802.15.4 authentication is not enabled. To protect against the reply attack, XBee uses a 32-bit frame counter that operates like a time-stamp and only resets when the network key is updated.

The DoS (denial of service) attack has two modes. The first is from inside when a node sends so many messages that the network freezes. It could happen for either the physical layer, application layer, or medium access control. The second mode is from outside and happens only at the physical layer. To keep the network from insider attacks, unauthenticated devices should not be allowed to join. For other cases, there should be a list of misbehaving nodes and then adding them to the black list. In case of monitoring misbehaving nodes, change the operating channel.

Another type of attack is attempting to acquire ZigBee link keys while the broadcast messages are encoded. The hacker can get the link key from a node by accessing it after a connection is established to the network. The link would be vulnerable if the network key is sent unencrypted over the air, or if the default values for the link are used. To prevent these attacks, the module must be re-configured before use and the network encryption should be enabled.

3.7. Network Topology

A ZigBee module could be configured to operate as either coordinator, router, or end-device. The network topology is defined by the connections made between these nodes. Every network must include one coordinator (only one, not more) and one or more routers and/or end devices. There are different network topologies such as star, cluster, tree, and mesh. Each topology has several advantages and drawbacks. Regarding our current application, the most compatible topology was star. The reason for selecting star was that each package goes through two hops to reach the destination node and the network formation is fast. The disadvantage of star is that when the number of transmitted packages per second increases more than a threshold, the coordinator could become bottlenecked. But regarding our algorithm for data interchange

between transmitter and receivers, a bottleneck will not happen in our network. Figure 5-a shows a network with one coordinator at the ITC side and four receivers on four sides of an intersection.

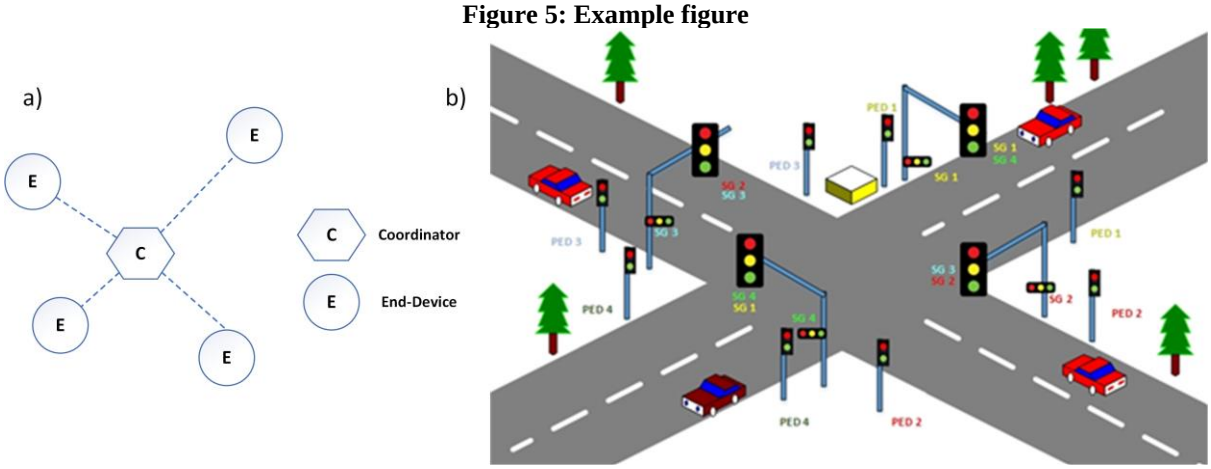
4. Design and Implementation

The design includes two parts: hardware, and software. Firstly, the software algorithm is discussed and then the hardware will be described.

4.1. Algorithm

Considering different tasks at both transmitter and receiver ends, there should be two different algorithms and software on each side. For instance, the transmitter that includes the coordinator ZigBee module is responsible for forming a network and maintaining its security against intrusion and safety for vehicles and pedestrians. First of all, the transmitter starts by accepting the necessary number of receivers defined by the operator but does not respond to join requests of invalid receivers. This mechanism is performed by a combination of AES coding, TrustFence, and the PAN-ID which is set on the system hardware by the operator before running the system. The transmitter continuously monitors the presence and status of the

Figure 5: Example figure



receivers and transmits the new status for traffic signal heads to the receivers. In case of failure in any receiver, like a missing receiver or vehicle red lamp burnout, the transmitter realizes it and asks the other receivers to start flashing mode. This will prevent traffic accidents for conflicting vehicle movements. On the other hand, the receiver starts with flashing mode and after reading the PAN-ID from the hardware that was set by the operator, looks for a valid network to join. After joining a valid network, it executes received instructions and in the meantime monitors the lamp status. In case of any failure such as isolation from a valid network or vehicle red lamp burnout, it switches to flashing mode and reports the error to the transmitter. The brief algorithm of transmitter and receiver is shown in Figures 6-a and 6-b.

4.2. Hardware- Transmitter

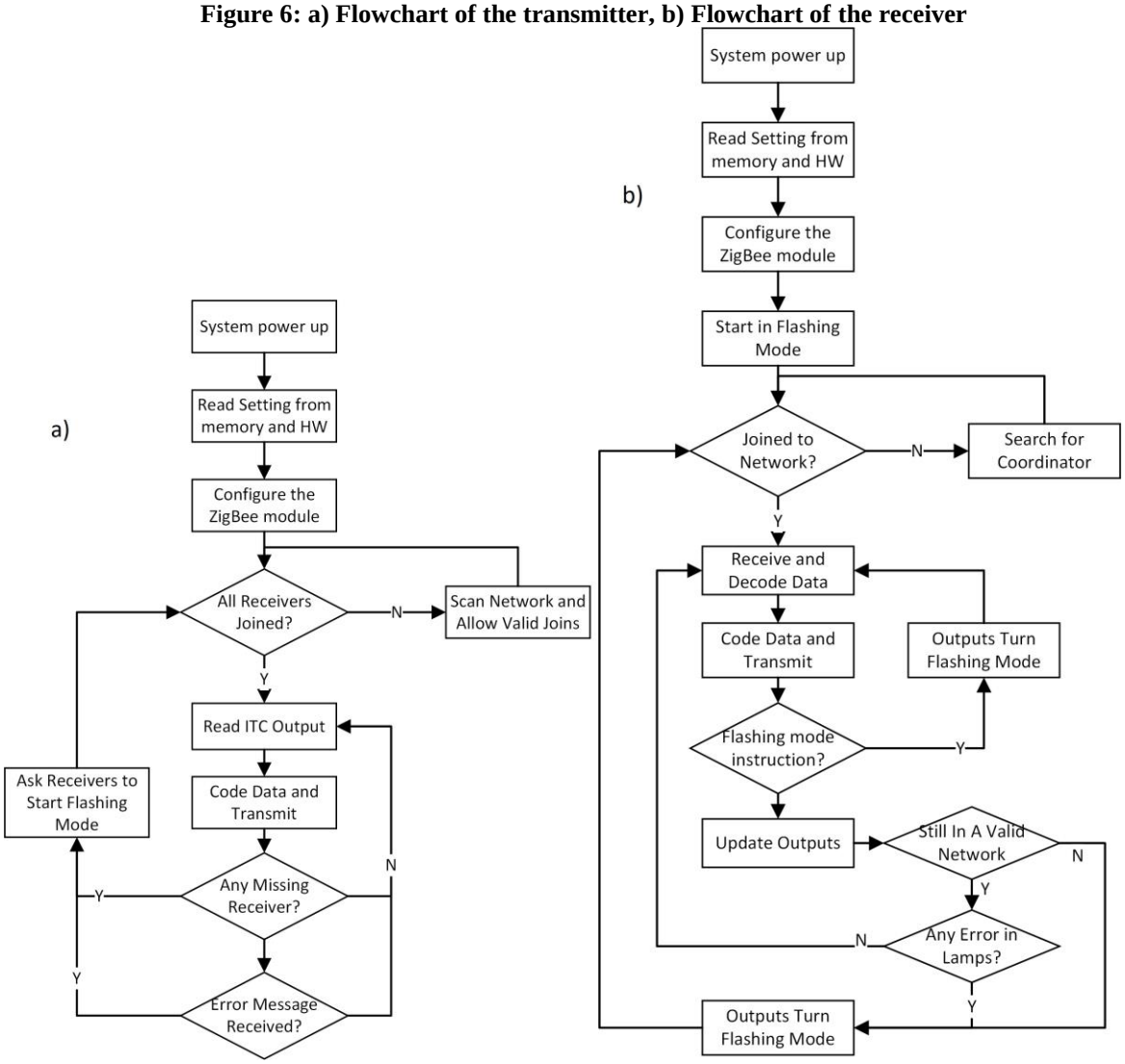
For ease of installation, the transmitter section is divided into two separate boards. The main and the radio board. The main is installed inside the ITC cabinet at the roadside fig 7-d. But, regarding the fact that the metal box of the ITC cabinet acts as a Faraday cage and weakens ZigBee radio waves, a small board is designed to be installed at the top of the traffic pole, figure 7-b. The radio board is connected to the mainboard via a network cable that transfers both power and data to be transferred to the receivers. The mainboard, figure 7-a, consists of a

dedicated switching mode power supply to provide +5 VDC and +3.3 VDC for different parts of the transmitter board. Also, it includes an LCD and push buttons to set different features of the system such as the number of inputs to be monitored and the number of expected receivers. In addition to settings in software, there is a hardware facility to set up the network dedicated for the current intersection. Each intersection in ITCs compatible with SCATS has a four-digit code that represents that intersection. Using four groups of four-bit jumpers, this number is set for each transmitter board. Using this code our transmitter neglects receivers of the adjacent network that are in the detectable range and so any interference is prevented. There is a section for RS485 communication to exchange data between the microcontroller and XBee module on the radio board. The transmitter section can include up to four sampling boards for reading the output of ITC.

4.3. Hardware- Receiver

The receiver board is shown in picture 9. In this board, several facilities have been considered to set up the requirement receiver conveniently and based on. The first step is setting up the Site-ID. Also, to keep track of the status of each receiver, the “module code” was considered for them. This code is defined using four jumpers representing four bits. Thus a code from 0 to 15 can be defined for each module as the receiver code in the network. Besides, each receiver can drive up to six signal groups, and there should facilities to assign each signal group to each

Figure 6: a) Flowchart of the transmitter, b) Flowchart of the receiver



output. This is done by six groups of four jumpers/bits as shown in figure 9. This number also represents the signal groups 1 to 16 that were read from the output of ITC. To increase safety in case of occurring any failure in the network, the color of the flashing mode for the outputs is adjustable. This is done using six jumpers, each representing outputs 1 to 6. If the jumpers are open-circuit, the output will be flashing yellow. But if the jumper is short-circuited, the output will be flash red. To decrease the size of the board no LCDs were used in the receiver section. Instead, three LEDs with different colors are used to display the momentary status of the receiver in the network, figure 8. The combination of these LEDs defines the current status of the system. This is explained in table 1.

Figure 7: a) Transmitter board, b) Radio board, c) Sampling board, d) ITC cabinet

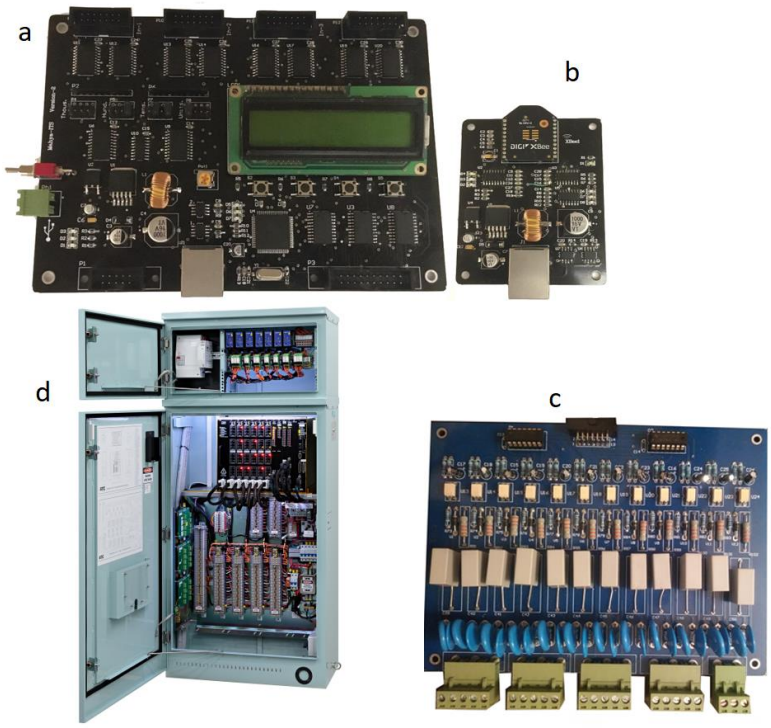


Figure 8: System indicator LEDs

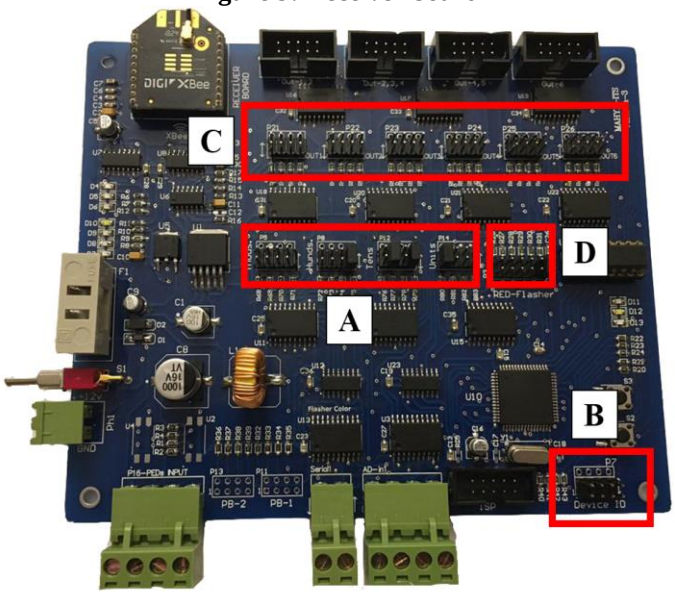
Table 1: Understanding current receiver status using indicator LEDs

Mode	LED Red	LED Yellow	LED Red	Definition
1	1	0	0	The module received a data packet, but this module was not the destination for this data packet
2	1	1	0	The module received a data packet and responded to that data packet. The network is operating in normal mode.
3	1	1	1	The module received a data packet and responded to that data packet. The network is operating in flashing mode.

5. Conclusion

Employing a wired connection between ITC and TSH leads to excessive cost and time required for implementation and maintenance. Besides, it can cause different faults in ITC operation and result in losing coordination in the network. A solution is replacing the wired connection with a safe and secure wireless connection, based on the latest generation of ZigBee protocol, i.e. XBee 3.0. This module has high flexibility in configuration and is equipped with TrustFence which provides outstanding security features compared to similar modules (Kumar, 2017). The hardware and software design was based on ITCs compatible with SCATS and thus several necessary standards were considered. This system was successfully tested with PSC-MK3 ITC and three receivers, each driving four traffic signal heads.

Figure 9: Receiver board



5.1. Performance

The production costs for the wireless modules are considerably low, compared to civil works required for preparing intersections for cabling and the price of the multicore cables. Moreover, the installation or maintenance time for the cableless method is less, compared to civil work at an intersection.

To test the performance of the system, it was installed on an intelligent traffic controller running a two-phase plan with pedestrian signal heads, and for some periods to maximize the number of transmitted packets, the controller was set to work on the flasher mode. During the test period, which was over three months, a total of 27 data packets were lost which belongs to the first receiver, located behind the wall and about 30 meters away from the transmitter. Also, this module was exposed to a noise generator placed beside it. Other receivers that were directly facing the transmitter in over 40 meters had no missing data packets, as shown in figure 10. The information of the traffic signal heads is sent every 250ms and if two consecutive packets are lost the system enters the flashing mode for safety measures. These lost packets did not affect the performance of the controller because did not cause the system to enter flashing mode. The system log shows that it did not enter the flashing mode due to connection failure.

5.2. Issues and Limitations

One of the limitations of this system is that the wireless module cannot exceed a specific speed in transmitting the wireless data. The frequency of data transmission depends on the size of

data packets. So, to keep the design practical we manually limited the transmission frequency to 4Hz or 4 data packets per second.

An important consideration in employing wireless devices is that they are vulnerable to jamming attacks. There are diverse methods to confront jamming attacks (Bensalem, 2019) (Rose, 2019) (Pirayesh, 2022). Regarding the module type used in this project, we used channel monitoring and changing as a secure way to overcome issues resulting from jamming attacks.

Figure 10: Lost data packets are represented by "error" (Err.)

5.3. Future Direction

The next step is upgrading the technologies used in both hardware and software of the ITC network. To achieve this goal, we are currently working on developing new methodologies of traffic signal management at the network level. For the hardware, an intelligent traffic controller integrated with ZigBee technology will be designed. It is expected that the new solution will remarkably enhance the power consumption, security, costs, and time required for production, installation, and maintenance of the ITC network, which helps the sustainable development of cities in the forthcoming years.

6. References

Ankita Bhutani, Preeti Wadhwani, 2019. Intelligent Transportation System (ITS) Market Size By Mode of Transport, *Global Market Insight*, 178.

Bensalem, M., Singh, S.K. and Jukan, A., 2019, December. On detecting and preventing jamming attacks with machine learning in optical networks. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

Danbatta, S.J. and Varol, A., 2019, June. Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

Department of Traffic and Marine Roads 2015, Traffic and Road Use Management - Volume 4 – Intelligent Transport Systems and Electrical Technology, Part 1: Traffic Signal Maintenance, April 2015. < https://www.tmr.qld.gov.au/-/media/busind/techstdpubs/Specifications-and-drawings/Specifications/4-Electrical-and-ITS/MRTS255.pdf?la=en > [Accessed 18 July 2022]

Digi.com. 2022. Zigbee 3.0 Security | Digi International. [online] Available at: <https://www.digi.com/support/knowledge-base/zigbee-3-0-security> [Accessed 9 May 2022].

Digi.com. 2022. Zigbee 3.0 Security | Digi International. [online] Available at: < https://www.digi.com/products/embedded-systems/digi-xbee/rf-modules/2-4-ghz-rf-modules/xbee3-zigbee-3> [Accessed 18 July 2022].

Kafi, M.A., Challal, Y., Djenouri, D., Doudou, M., Bouabdallah, A. and Badache, N., 2013. A study of wireless sensor networks for urban traffic monitoring: applications and architectures. *Procedia computer science*, *19*, pp.617-626.

Kandris, D., Nakas, C., Vomvas, D. and Koulouras, G., 2020. Applications of wireless sensor networks: an up-to-date survey. Applied System Innovation, 3(1), p.14.

Kumar, N.R., Bhuvana, C. and Anushya, S., 2017, February. Comparison of ZigBee and Bluetooth wireless technologies-survey. In *2017 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 1-4). IEEE.

Nellore, K. and Hancke, G.P., 2016. A survey on urban traffic management system using wireless sensor networks. *Sensors*, *16*(2), p.157.

Pirayesh, H. and Zeng, H., 2022. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

Qi, L., 2008, August. Research on intelligent transportation system technologies and applications. In *2008 Workshop on Power Electronics and Intelligent Transportation System* (pp. 529-531). IEEE.

Rose, S.H. and Jayasree, T., 2019. Detection of jamming attack using timestamp for WSN. *Ad Hoc Networks*, *91*, p.101874.

Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. *Computer networks*, *52*(12), pp.2292-2330.

Zandi, F. and Tavana, M., 2011. An optimal investment scheduling framework for intelligent transportation systems architecture. *Journal of Intelligent Transportation Systems*, *15*(3), pp.115-132.

Zhang, J., Wang, F.Y., Wang, K., Lin, W.H., Xu, X. and Chen, C., 2011. Data-driven intelligent transportation systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), pp.1624-1639.

Zhang, S. and Zhang, H., 2012, August. A review of wireless sensor networks and its applications. In *2012 IEEE international conference on automation and logistics* (pp. 386-389). IEEE.

Zhou, J., Li, C. and Zhang, Z., 2011, October. Intelligent transportation system based on SIP/ZigBee architecture. In *2011 International Conference on Image Analysis and Signal Processing* (pp. 405-409). IEEE.