Original research paper

A Survey on cybersecurity of traffic signal systems

Dharani Chandran[1], Yunpeng Zhang[1]*, Liang-Chieh Cheng[2]

[1]*University of Houston, Department of Information & Logistics Technology, Houston, U.S.A.*

[2]*University of Houston, Department of Construction Management, Houston, U.S.A.*

Abstract

Traditional standalone traffic signals are being replaced by adaptive traffic signals, which automatically adjusts the control parameters, and revises the signal plans are becoming an integral part in the modern road transport infrastructure. These advancements that are based Cyber-Physical systems come with a lot of weakness that could be easily exploited for example some of these systems are used without any encryption for communication between a central traffic control management system and field traffic signal control units, allowing an attacker to directly change traffic signal indications. Vulnerabilities like this could allow anyone to take complete control of the traffic control devices and could cause a traffic mess. Many literatures have been published in the recent years explaining various strategies to prevent the attack against adaptive traffic signals system. In this paper, we present a survey summarizing relevant works in the field of traffic light cyber security. This survey discusses and organizes different methods on securing against a series of major security weaknesses in traffic light systems highlighting the importance of a defense system and their impacts on them.

Keywords:

Cybersecurity, traffic signal system

* Corresponding author. Assistant Professor, Department of Information and Logistics Technology, College of Technology, University of Houston-Main Campus, yzhang119@uh.edu

1 Introduction

Traffic signal systems have evolved from series of standalone pieces of technology coordinated through synchronized time clocks to a series of sophisticated programs running on a series of connected computers networked together using both wired and wireless technologies. While new technologies have greatly enhanced how traffic signals work and efficiently operate, it has also increased the exposure to a lot of cyber security threats. Recent studies performed on the security of traffic lights, discovered a number of security vulnerabilities existing in the system, these researchers demonstrated that they were able to successfully compromise the security measures used by agencies and access the agency's traffic signal system network. Their attacks showed that an adversary could gain access to the traffic signal system, potentially disrupting service, compromising safety, and altering operations of the traffic signal to provide advantages to unauthorized users.

The nation's roadway network is connected not only with asphalt and concrete, but also by traffic control systems which ensure the safety and mobility for roadway users. These traffic control systems are composed of traffic signal controllers, dynamic message signs, roadway detectors and sensors, road weather information systems, weigh-in- motion systems, etc. Over 20 years, transportation industry has embraced Intelligent Transportation Systems (ITS) to reduce crash rates, traffic congestion, vehicle emissions, and increase safety, reliability, and mobility for all transportation modes. Table 1 summarized enabling technologies in ITS. The team also attached a national intelligent transportation system architecture, a national ITS architecture layers, and a connected vehicle reference implementation architecture as Appendix 2, 3 and 4. According to previous studies, there are more than 20 types of ITS subsystems such as traffic management systems, transit management systems, freight management systems, emission management systems, archived data management systems, etc. (USDOT, 2005; Puget Sound Regional Council, 2006; Berenson, 2012).

While to adaption from standalone systems to advanced, adaptive systems are being rapidly implemented, they also open to new possibilities for hackers to utilize it for the personal gains. A researcher from IOActive was able to get into the traffic signal system with the help of devices which costed him just $100, this explains the state of the current system and necessity to react and address those problems.

Table 1 Summary of enabling technologies in ITS (Qureshi and Abdullah, 2013)

Technologies	**Types**
Communication	Wireless (Cellular or Wide Area) Wire line (Coaxial or Fiber Optic)
Data storage and processing	Compact Disc, Magnetic storage, Media Magnetic stripe cards, hard disks and data cartridges, smart cards
Database management systems	Data Warehousing, Expert Systems
Information display	Cathode ray Tubes (CRTS), LCDs, Variable message sign
Location	Dead reckoning, Map matching, GPS, Beacon based Vehicle Location
Sensors	Inductive Loops, Infrared Beams, Microwave (RADAR), LIDAR, Vision-based Sensors, Acoustic scanning Laser
Actuator	Gates and Displays

1.1 Traffic signal setup:

A traffic monitoring sensor node typically comprises of the modules as given below, the Fig 1 gives a outlook of the setup and flow of information in the traffic control system.

A. Sensors—which acquires data.

A sensor is a device that transforms a physical process into an electrical signal. They are usually implanted underneath the surface and are used to detect a change in the earth's magnetic field when a vehicle passes over its measured area of influence. They generate useful traffic information such as number of cars, speed and length of the vehicles, based on processing of the sensor data. The information is then sent to the nearest intersection control agent over a wireless network. Magnetometer is commonly used for measuring the magnitude and direction of the earth's magnetic field. Device used to detect changes in the earth's magnetic field within the vicinity of the instrument. [1]

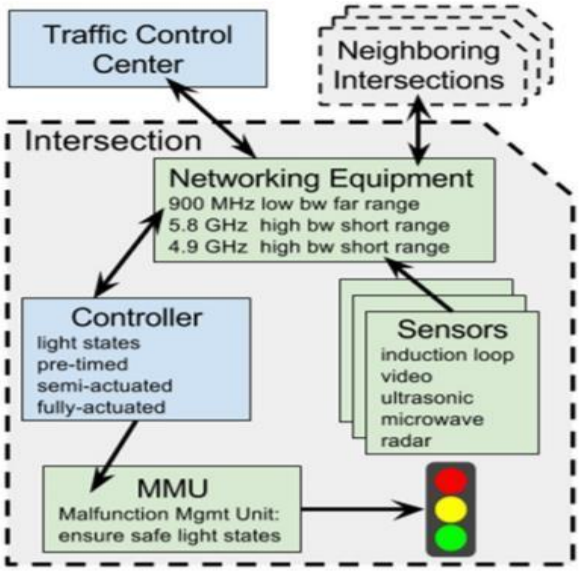

Fig1. Components of an adaptive traffic signal

B. A processing and control module which processes the local data and stores it.

They carry out the necessary data processing and radio communication control. The controller uses input from detectors, which are sensors that inform the controller processor whether vehicles or other road users are present, to adjust signal timing and phasing within the limits set by the controllers. [2]

C. A radio module—this module is for wireless data communication.

D. A power module—which is module is for energy supply.

E. The MMU (Malfunction Management Unit)

MMU is the failsafe operator on the system and ensures that the lights are not put into an unsafe state (such as for Red and Green at the same time), and the lights are then adjusted using the information gained from the induction loops in the road (and which senses cars as they pass over it). If control can be gained to the MMU, and allow for access to the controller, the lights can be compromised to go into incorrect states, or to stay at steady red (and cause a grid lock within a city). Within the MMU controller board, the researchers found that by connecting a jumper wire, the output from the controller was ignored, and the intersection put into a known-safe state.

F. Wireless Sensor Networks

The physical architecture of a wireless sensor network consists of several Sensor Nodes (SN) and a single Access Point (AP). The raw sensor signals are first processed by the processor in the sensor node to extract some useful information. The output of this initial sensor node-based processing is transmitted to the access point either through a direct communication with the access point or a multi-hop communication across other sensor nodes. Eventually, the access point processes the data collected from all the sensors in the network to extract more information, places this information into some meaningful format and sends it to the end user or some other control system. [3-6]

1.2 Working of an adaptive model

Sensors are implanted along the road which detect the number of vehicles and traffic density at that junction, once the detections are made, each wireless sensor sends time-stamped detection event data to a nearby access point or repeater. The radio communications between a wireless sensor and its communicating access point or repeater are two-way, allowing the sensor to receive commands and data as well as transmit data and status information. Each wireless sensor is uniquely addressable so its data can be independently collected and its operation independently controlled and monitored. The controller upon receiving the information will decide whether to alter the signal length and thus efficiently decreasing the wait time at the intersections [7]. Fig. 2 gives us a visual representation of the traffic signal setup comprising of the modules discussed above.

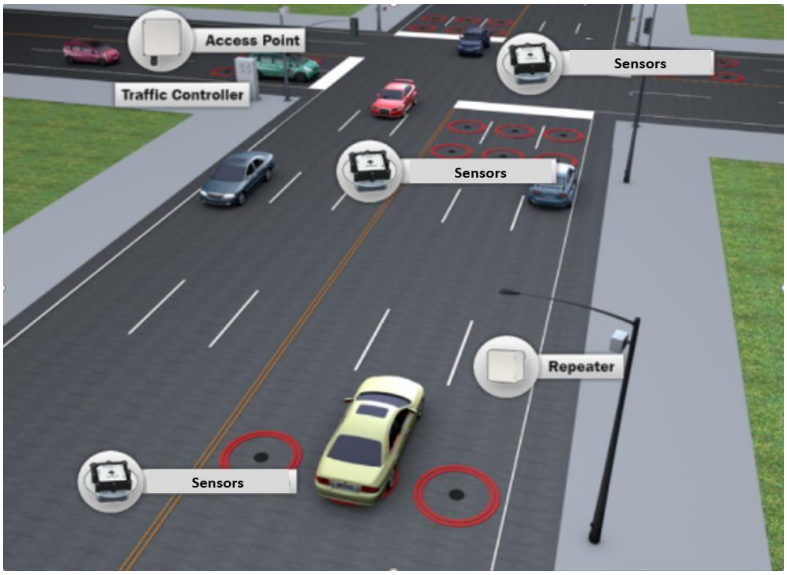

Fig. 2: Setup of an adaptive traffic control

1.3 Objectives and contributions of the research

The objective of this paper is to examine the most relevant, recent publications on adaptive traffic light systems. Our research studies the critical technologies associated with traffic light systems and the security aspects of these published work. The present paper is aimed at introducing to the future researchers: 1) the existing concepts in this field, and 2) the importance of developing and implementing an effective security element for adaptive traffic light system.

2 Critical concepts regarding cybersecurity of traffic signal systems

The current traffic signal systems rely on sensor technologies to manage the actuation and timing of traffic signals. The sensors are susceptible to various attacks. The following list summarizes the most common types of attacks.

2.1 Analyzing vulnerabilities of traffic light system

A. **Spoofed, altered or replayed routing information** May be used for loop construction, attracting or repelling traffic, extend or shorten source route.

B. **Selective forwarding** in this attack, the attacker prevents the transmission of some packets.

They will be removed later by the malicious node.

C. **Hello flooding attack:** Acknowledgement spoofing in this attack, the attacker tries to convince the sender that the weak link is strong or that a dead node is alive. Therefore, all packets passing through this link or this node will be lost. [8]

D. **Denial-of- Service Attacks:** A denial-of- service (DoS) targets the availability and capacity reduction of network services. Physical constraints of the sensor networks and the nature of their deployment environment, make them vulnerable to DoS attacks more than any other type of network Layer Attack Defense.

E. **Sensor node Compromise**: Sensor networks consists of hundreds or thousands of sensor nodes. Adaptive traffic controllers will soon involve having such a setup. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical

attack. Attackers can either introduce their own sensor nodes or could compromise a single node to hold access to the entire network. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks—for example, falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. [9] The Table 1 below gives a view on list of possible attacks at various layers.

Table 1. Vulnerabilities at various layers and corresponding defense techniques

Layer	Attack	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring, redundancy
	Wormhole	Authentication, probing
	Hello Flood	Authentication
Transport	Session Hijacking.	aggregation data
	SYN flooding	Package authentication
	Data Corruption.	Authentication

2.2 Consequences of Cyberattacks:

A. **Privacy issue** - Networks of traffic light systems aren't used only to regulate traffic flow; the sensors can be also used to count vehicles in a specific area of the city or to track the movement of vehicles by detecting the same vehicle with different sensors located in different positions in a metropolitan area. This data could allow bad actors or governments to track specific vehicles violating the users' privacy.

B. **Denial-of-service (DoS)** attack on controlled intersections that could cause a traffic jam. As explained by the researchers the attackers could set the all lights to red or trigger the MMU to take over by attempting an unsafe configuration, this last case is serious because need a physical intervention of personnel to restore a normal situation.

C. **Traffic Congestion** manipulating timings of an intersection relative to its neighbors with repercussion for the entire traffic infrastructure. Such attacks have a significant financial impact on the community targeted as demonstrated by numerous studies.

D. **Light control** for personal gain, as explained by researchers' lights could be changed to red in coordination with another attack in order to cause traffic congestion and slow emergency vehicle response.

3 Recent researches on Traffic light security

3.1 A Secure Architecture for Traffic Control Systems with SDLC Protocols:

Reference [10] discusses concerns on security in an intelligent traffic system (ITS) that utilizes synchronous data link control (SDLC) protocol. SDLC is a legacy protocol which was primarily used for remote communication on wide-area networks. It is now replaced by (High-Level Data Link Control) HDLC protocol, but still SDLC is widely used across many traffic control systems and several derivative protocols are widely used in its domain. The SDLC is designed to deliver data from a primary device to many secondary devices. The secondary devices cannot initiate commutation with the primary in a SDLC protocol. SDLC primarily works on poll and response model.

The paper proposes an architecture(Fig.3) in which it uses message integrity, authentication of the node and digital signatures using public key infrastructure (PKI) for communications between the actuated signal Controller(ASC) and the controlled devices (malfunction management unit, terminal facility bus interface units). To overcome the threat posed by the legacy equipment's in ASC/SDLC the papers introduces a master device between the ASC and the controlled devices which decrypts the commands, checks error and then sends commands to the terminal services. For a wide area communication, to secure the communication the author introduces a secure communication adapter (SCA) between the ASC and the communication network as shown the fig 3. The author also discusses the use of secure algorithm in this proposed architecture and demonstrates its effectiveness by a series of stimulation results. [11]

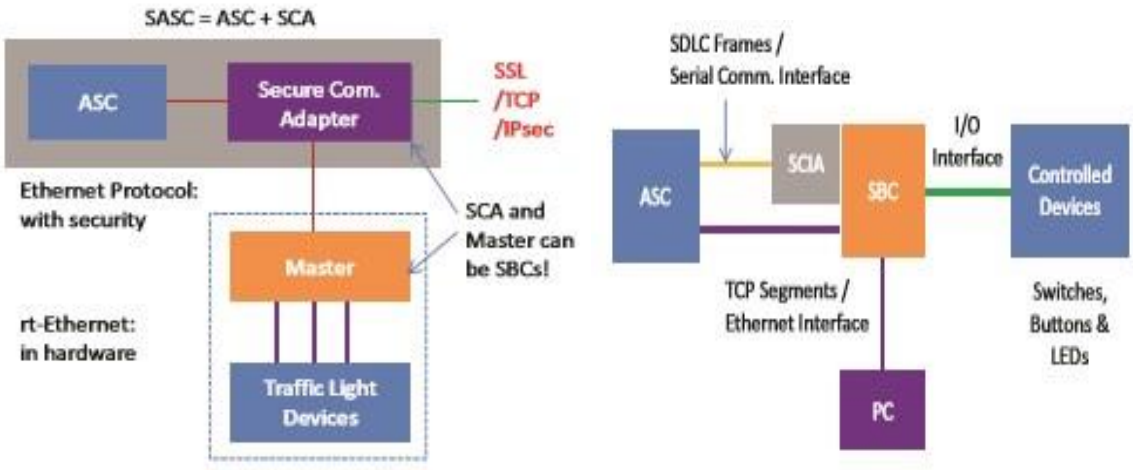

Fig.3 The architecture of the proposed secure ASC contains a SCA

3.2 Disrupting Adaptive Traffic Lights Cycles through Selective Jamming Attack

Reference [12] discusses about various jamming attacks by the signals from the vehicles to traffic light system. These attacks would lead in an incorrect load estimates causing to disrupt the effectives of the adaptive traffic light system. The author considers impact of stealthy attacks on adaptive traffic lights in particular. The paper starts with the model that introduces us about the effect of traffic lights adaptation by learning the flow of vehicles. The paper considers a single four-way intersection with two-lanes in each direction as shown in fig. The author evaluates the effect of the exposed attacks using SUMO simulations under various types of attack scenarios and for different metrics of damage and cost.

- Uniform Random Attack with a Probabilistic Emission Model:
- Uniform Random Attack with a Deterministic Emission Model:
- Isolated Random Attack with Deterministic Emission Model:
- Uniform Random Attack with Deterministic Emission Model with smoothing functions
- Targeted Random Attacks with Deterministic Emission Model:

With the above-mentioned scenarios, to access the impact of the exposed jamming attacks on the performance of adaptive traffic lights, the author follows the attack potency, which is given by the following formula, π = Damage /Cost. With this equation, the authors calculate the damage as the difference in trip times that vehicles experience due to the attack. The paper concludes

that both system-wide and targeted attacks do have a significant impact on the average trip times. The most potent attack for a system-wide attack occurs at a similar rate of attack as a targeted one. We have shown that an attacker mounting an attack on one segment can increase the average trip time more when compared with a similar strength attack on the entire system. Similarly, a driver who seeks to attack opposing lane groups is able to reduce their own trip time. With this research, the author introduces us to the basic structure for jamming attacks and layers foundation to for research in more optimized ones in our future work. [13]

3.3 Green Lights Forever: Analyzing the Security of Traffic Infrastructure

Reference [14] explains the security flaws in the existing control traffic infrastructure. The anatomy of traffic intersection contains sensors which are used detect the traffic change. Controllers are used to read the data collected by the sensors; it receives vehicle detection signals and uses those, along with preset timing plans, to determine when the lights should change. Malfunction Management Unit, also known as the Conflict Management Unit. The MMU is a hardware module used to prevent faults in the traffic light system. It watches the outputs of the controller for invalid control signals. The MMU determines validity with a configuration circuit board. These things are hand-soldered by road agency personnel. Where each connection is a whitelisting of possible light states. If the MMU detects an invalid state, it overrides the controller and takes the system into a failsafe state. The traffic signals go to blinking red lights. Communications takes paces between the traffic lights or between a traffic light and the control center using radios.

- The 900 MHz communication radios have no encryption and used default username and password which is easily available over internet.
- The 5.8 GHz radios were detectable from laptop but were not able to connect. These radios also had no encryption enabled and used default username and password Using the radio by the same vendor allowed to connect to the network and thus providing access to all intersections on the network.
- Controllers didn't have an access control in place. It has an FTP server where a database file with settings can be accessed. It VxWorks runs on the controller and has debug port open. The vendor created a program made for remotely operating controllers through this protocol. It was easy to sniff with Wireshark and we were able to reverse engineer how several commands mapped to button presses on the front panel of the controller. By creating a library of controllers into a traffic controller shell, setting on the controllers were able to modify. Thus, changing the traffic lights. [15]

3.4 Research conducted by IOACTIVE Labs

In reference [16], the researcher launched the attack from a drone flying at over 650 feet, and it worked and added that theoretically, an attack could be launched from up to 1 or 2 miles away with a better drone and hardware equipment. The researchers purchased an access point from Sensys Networks at a cost of about

$4,000. The access point acquired by the researcher are compatible with all the sensors used by the Sensys to monitor the streets worldwide. The access point intercepts data sent by sensors. It was found that all communication is performed in clear text without any encryption nor security mechanism. Sensor identification information (Sensorid), commands could be observed being transmitted in clear text. Because of this, wireless communications to and from devices can be monitored and initiated by attackers, allowing them to send arbitrary commands, data and manipulating the devices. [16] Key findings in the experiment:

- No authentication ´Sensors and repeaters can be accessed and manipulated over the air by anyone, including firmware updates.
- AP doesn't authenticate sensors, just blindly trusts wireless data
- Firmware updates not encrypted nor signed ´Anyone can modify a firmware and get it updated on sensors and repeaters. [3]

3.5 Security in Sensor Network Based SCADA System for Adaptive Traffic Signal Operation

Reference [17] comes up with an idea to provide security to an integrated adaptive traffic system. Though the main goal of the paper is to deliver an efficient and intelligent traffic adaptive system, It also talks about a way to secure them.

The paper uses fuzzy logic for decision making based on the real-time traffic data. The system considered for collecting data is through wireless sensors deployed in intersections. The sensors communicative with bases stations though wireless communication and uses wired network to communicate between base stations, the controllers are all Base stations.

In this approach sensors are deployed in in the traffic signal intersections. Sensors communicate with the base station which is placed locally. Base station uses fuzzy logic to manage the local traffic signals. Base stations also communicate with other base stations through the wired network to effectively manage all the traffic lights in the region for smooth traffic flow. All of the base stations are controlled in a region through a controller, and the controller is controlled by the SCADA system.

The model considers that the attack can happen at any of the layers and any of devices in the setup. The first layer of security suggested is that output from the fuzzy logic are check of data integrity. Any message that doesn’t satisfy the integrity check is discarded at that point. The next defense mechanism introduced is IDS in the SCADA system. Any intrusion pattern that would match with the IDS signatures are identified at

real-time. The next approach considered is the Key Computation and Communication. The paper proposes Centralized approach that would reduce the overhead to the sensors and providing authority to the SCADA. The author suggests that with some improvement, this system could thwart attackers from getting onto the system. [18]

4 Conclusion

This paper introduced the current practice in setting up an adaptive traffic signal and the view on the state of cybersecurity practices on those systems. In our evaluation, the existing setups of traffic light systems, while bringing in a significant advantage in traffic control over the old systems, do not protect the control center and devices from cyber-attacks. Unless effective security contorts are placed, the existing vulnerabilities could be easily exploited by attackers, who may only have little knowledge of the sophisticated traffic manage systems. The present paper provides a basic understanding of the deficiencies in the traffic light system and seriousness for traffic management stakeholders and researchers to act swiftly to address those problems.

References

Losilla, Fernando, et al. "A comprehensive approach to WSN-based ITS applications: A survey." *Sensors* 11.11 (2011): 10220-10265.

Al-Nasser, Faisal Ahmed, and Magdi S. Mahmoud. *Wireless sensors network application: a decentralized approach for traffic control and management*. INTECH Open Access Publisher, 2012.

Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." *Computer networks* 38.4 (2002): 393-422.

Cerrudo, C.: 'Hacking US traffic control systems', available at: https://www.defcon. org/images/defcon-22

Ghena, B., Beyer, W., Hillaker, A., et al.: 'Green lights forever: analyzing the security of traffic infrastructure'. Proc. Eighth USENIX Conf. Offensive Technologies, 2014

Laszka, A., Potteiger, B., Vorobeychik, Y., et al.: 'Vulnerability of transportation networks to trafficsignal tampering'. Seventh ACM/IEEE Int. Conf. Cyber-Physical Systems (ICCPS), April 2016

Jacobsen, Alan. "Wireless Technology and a New Approach to Vehicle Detection." IMSA Journal (n.d.): n. pag. Web.

Maleh, Yassine, and Abdellah Ezzati. "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks." *arXiv preprint arXiv:1401.1982* (2014).

Chan, Haowen, and Adrian Perrig. "Security and privacy in sensor networks." *computer* 36.10 (2003): 103-105.

Ming Yu, Ziyuan Cai, L Tung, A Secure Architecture for Traffic Control Systems with SDLC Protocols, A Secure Architecture for Traffic Control Systems with SDLC Protocols, 14-17 Oct. 2012

Yu, Ming, Ziyuan Cai, and Leonard Tung. "A secure architecture for traffic control systems with SDLC protocols." *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*. IEEE, 2012.

Heather Hinze, Michael Ruth, Mina Guirguis, Disrupting Adaptive Traffic Lights Cycles through Selective Jamming Attacks, Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st.

Hinze, Heather, Michael Ruth, and Mina Guirguis. "Disrupting Adaptive Traffic Lights Cycles through Selective Jamming Attacks." *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*. IEEE, 2015.

Branden Ghena, William Beyer, Allen Hillaker, etc. *Green Lights Forever: Analyzing the Security of Traffic Infrastructure,* Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14), August 2014: 1-10

Ghena, Branden, et al. "Green Lights Forever: Analyzing the Security of Traffic Infrastructure." *WOOT* 14 (2014): 7-7.

"Hacking US (and UK, Australia, France, etc.) Traffic Control Systems." IOActive. N.p., n.d. Web. 30 Apr. 2014.

Biswajit Panja, Atul Prakash, Priyanka Meharia, Security in Sensor Network Based SCADA System for Adaptive Traffic Signal Operation, Collaboration Technologies and Systems (CTS), 2012 International Conference on, 21-25 May 2012

Biswajit Panja, Atul Prakash, Priyanka Meharia, Security in Sensor Network Based SCADA System for Adaptive Traffic Signal Operation, Collaboration Technologies and Systems (CTS), 2012 International Conference on, 21-25 May 2012

Panja, Biswajit, et al. "Security in sensor network based SCADA system for adaptive traffic signal operation." *Collaboration Technologies and Systems (CTS), 2012 International Conference on*. IEEE, 2012.