CYBER ATTACKS ON SCADA BASED TRAFFIC LIGHT CONTROL SYSTEMS IN THE SMART CITIES

Cevat Özarpa, İsa Avcı*, Bahadır Furkan Kınacı, Suat Arapoğlu, Seyit Ali Kara,

Karabuk University, Department of Mechanical Engineering, Karabuk, Turkey- cevatozarpa@karabuk.edu.tr
Karabuk University, Department of Computer Engineering, Karabuk, Turkey - isaavci@karabuk.edu.tr
Karabuk University, Department of Rail Systems Engineering, Karabuk, Turkey - furkankinaci@karabuk.edu.tr
Yakakent Cad. Yakakent Sitesi Defne Apt., Yakacık, Kartal, Istanbul, Turkey- suatarapoglu@gmail.com
Karabuk University, Department of Mechanical Engineering, Karabuk, Turkey - drseyitalikara@gmail.com

KEYWORDS: Cybersecurity, Cyber-Attacks, Cyber Risk Analysis, Smart Traffic Light System, Smart Traffic.

ABSTRACT:

There are regular developments and changes in cities. Developments in cities have affected transportation, and traffic control tools have changed. Traffic signs and traffic lights have been used to direct pedestrians and vehicles correctly. Traffic light control systems are used to ensure the safety of vehicles and pedestrians, increase the fluency in traffic, guide them in transportation, warn pedestrians and drivers, and regulate and control transportation disruptions. In order to facilitate people's lives, it is desired to control the traffic components autonomously with the developments in autonomous systems. Cyber threats arise due to the active use of the internet and signals or frequencies in the use of modules that will provide communication with traffic lights, traffic signs, and vehicles, which are traffic components at the inter-sections of many roads in the control of central systems. The study is limited to smart traffic lights, which are traffic components. If we examine the cyber-attacks, we can see that Malware Attacks, Buffer Overflow Attacks, DoS attacks, and Jamming Attacks can be made. Network-Based Intrusion Detection Systems and Host-Based Intrusion Detection Systems can be used to detect and stop Malware Attacks, Buffer Overflow Attacks, DoS attacks, and Jamming Attacks. Intrusion detection systems tell us whether the data poses a threat or does not pose after the data passing through the system is examined. In this way, system protection is ensured by controlling the data traffic in the system.

1. INTRODUCTION

Due to the development of autonomous systems, autonomous systems have started to be used in traffic signs and traffic lights. With the use of smart traffic lights, cyber vulnerabilities have emerged in the system. Wired and wireless managed system has the weaknesses of wired and wireless systems. People who have infiltrated the system may confuse the system. Excessive traffic congestion may cause delays or accidents. These systems, which facilitate traffic control, make it difficult to control in cyberspace. Using the benefits of technology makes human life more manageable. If smart traffic light systems that will save time in traffic are protected from cyber-attacks, the traffic will become more fluid. Much time is spent in traffic in crowded cities. Especially in big cities, there is a need for smart traffic light systems.

It is a fact that cyber-attacks already offer an opportunity in terms of anonymity and deniability. In addition, it is difficult to determine who and by whom these attacks are financed, and which countries are behind these attacks. For this reason, it is very difficult to identify risks and threats in cyberspace and take precautions against them. In such an environment, it is no longer mentioned about providing absolute cybersecurity, instead, it is aimed to keep cybersecurity risks at manageable and acceptable levels (Özarpa et al., 2021). It is accepted that being in an open and connected environment such as the Internet will bring some risks along with increased inaccessibility. With a holistic approach involving all stakeholders, be prepared for cyber incidents by managing these risks and ensure the continuity of these events by eliminating the least damage is essential (Avcı et al., 2020).

The smart city concept includes energy infrastructure, traffic management, waste management, healthcare, transportation, water supply, and other services. Thus, there is interaction between service providers and citizens in a smart city. In a smart city, information, and communication technologies (ICT) are used to improve the quality, productivity, and consistency of urban services. In addition, smart cities aim to reduce costs and resource consumption and improve communication between citizens and the government. Research on smart cities started in the 2000s and many definitions were made for smart cities. For example, a smart city can be defined as a combination of reliable infrastructure, data transfer quality, and corporate infrastructure. Nijkamp et al. noted that a smart city can be created under certain conditions. Human and social capital and business in classical and modern communication infrastructure should provide sustainable economic support and high value of life. In addition, it is necessary to manage natural resources wisely through leadership (Nam, 2011).

In this study, smart traffic lights in smart cities and cyber-attacks on these systems will be detected. In addition, all systems will be examined, and their systematic structure will be given. In addition, necessary precautions will be given.

2. TRAFFIC LIGHT SYSTEMS TECHNOLOGY

Traffic is a big problem in crowded cities. In crowded cities, roads are bustling. Many foreign drivers on the roads create problems such as going in the wrong lane or turning on the wrong road. The excess of novices or foreigners in traffic causes delays and accidents in traffic. In order to prevent this situation, big cities include the components that smart cities should have. With the development of smart cities, it is aimed to

minimize or even eliminate accidents, delays, traffic jams, and instability in traffic at the intersections of many roads for smart traffic systems, which are the essential components of smart cities. Fluency is essential in the movements of vehicles. Synchronization is very important for traffic lights and traffic signs that have more than one intersection. Intelligent traffic lights system can be examined under two separate headings. These are:

- Fixed time smart traffic lights system,
- Density-based smart traffic light system.

2.1. Fixed Time Smart Traffic Lights System

They are systems that work as red, yellow, and green lights turn on alternately at certain time intervals. Transition priority is set according to fixed times. Pedestrians and vehicles switch according to the colors of the traffic lights adjusted for the time on the road. It is unresponsive in emergencies. Since there is no mobility in emergencies, drivers and pedestrians in traffic prioritize the emergency as a humanitarian.

2.2. Density-Based Smart Traffic Light System

It is used on roads where traffic density differs. It is a very efficient system at points where fixed-time smart traffic lights are insufficient. It is a system where the transition times can be adjusted in the directions where the traffic density is high, and the transition can be provided for more time. In case of emergency, pass priority is provided by the system. Drivers or pedestrians do not need to take any action. A density-based smart traffic light system can transmit signals from pedestrians and vehicles to the main center using routers. Directions are made for the most fluent traffic situation by using previously installed scenarios within the servers. Areas can apply data coming from the main center with the router, ethernet, and LAN connections within themselves. This situation is shown in Figure 1.

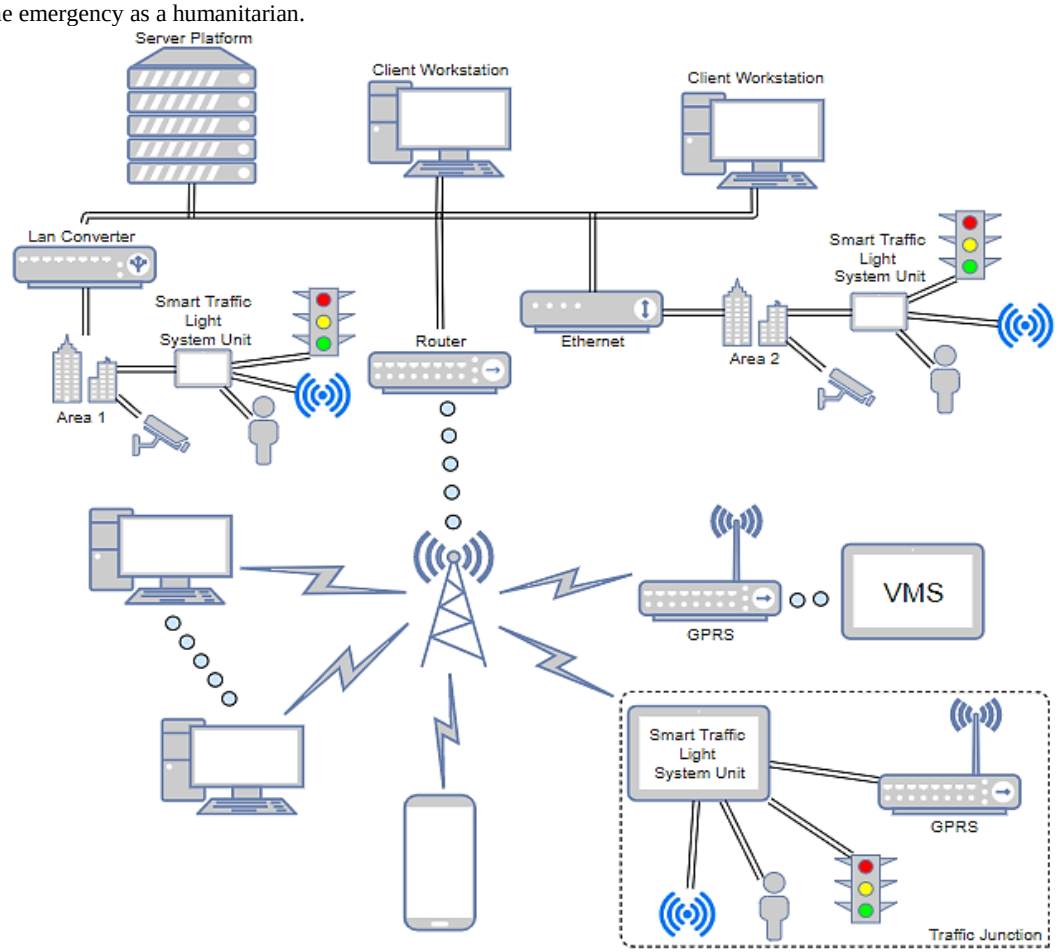

Figure 1. Density-based smart traffic light system scheme.

3. CYBER-ATTACKS ON TRAFFIC LIGHT SYSTEMS

The smart traffic lights system makes our life much easier and will make it even more manageable in the future. However, since there is no security system in the cyber world, this system has vulnerabilities (Comert et al., 2018). The attacks that can be made on the smart traffic lights system are Buffer overflow, DDoS, Malicious Code, and Jamming attacks. The threats and effects of those attacks have shown in Table 1.

If cyber-attacks are not prevented, delays may occur in traffic. Cyber-attacks can also cause misdirections and accidents in traffic. This puts human life in danger. In emergencies, the system can be entirely or temporarily disabled, confusing emergencies. The details of the attacks are mentioned in the continuation of the section.

3.1. Buffer Overflow

The density of traffic on gateways acting as central points of connection to the internet can increase the network load on specific routes, causing saturation of connections and buffer overflows. Also, if the routing protocols cannot handle the network load, the traffic overload on the routers will affect the performance of the overall network backbone. Buffer overflow attacks cause slowdown due to memory overflows. Akram Hakiri et al. has been found to decrease from 800 kB/s to 697 kB/s. However, increasing the number of wireless routers helps to distribute the load among them. Reducing the problem by increasing the number of routers does not increase the capacity of the network (Hakiri et al, 2015). Heuristic algorithms should consider both the wireless channels and the routing algorithm (Kumar et al., 2009), (Lee, 2008).

3.2. DDoS

If a system with the responsibility to request gets too many requests, the system will not accept. These systems are like a place that has a door (Javaid et al., 2018). If too many people entry to the place same time, nobody can pass through one door. In the attacks, too many fake signals are produced and sent to the target. Too many signals make the target system unable to respond. The IoT network at the smart traffic light creates an environment for DDoS attacks as the network has low power and storage and is dealing with a significant amount of mutable data at the same time. In smart traffic light systems, this happens via radio frequencies. The vulnerability was discovered when the European Telecommunications Standards Institute included a radio frequency band used by the EU for Intelligent traffic light systems (Kang et al., 2018).

3.3. Malicious Code

Malicious code is used to interfere with the working state of the computer. Hackers can stop the system from operating or render them unusable. In Traffic Light Systems, Malicious Code can disrupt the use of systems. Malicious code can be loaded into the system via wired or wireless connections. Installing Malicious code can cause incorrect indicators to work on smart traffic lights. Accidents and injuries will happen in case of traffic jams (Vassalo et al., 2018). The fact that the system has wired connections shows that the system can be infiltrated using city networks. Since the connection between vehicles and traffic signs is wireless, it is possible to intervene in the status of traffic signs using wireless data transfer into the system using wireless communication (Zheng et al., 2019).

3.4. Jamming Attack

Jamming attacks are a type of attack that intentionally sends a radio signal to disrupt packets in the wireless transmission medium, thus disrupting or completely blocking the communication of nodes, and is an important threat to wireless sensor networks (Avcı et al, 2017). It is called a kind of Denial-of-Service attack that prevents communication to another channel by occupying the channel on which they are communicating (Sedjelmaci et al., 2018).

4. PROTECTION TO CYBER THREAT

Network intrusion detection systems and firewalls are used for attacks on systems. In preventing attacks after detection, firewalls can control the flow of communication, and network IDSs monitor communication to detect potential attacks. Detection of attacks on systems has, in practice, been primarily delegated to sensors such as network intrusion detection systems.

Possible Attacks	Threat	Effect
Buffer OverFlow	Replacing system files	Loss of system control
DDoS	It prevents the system from transmitting data and detecting by sensors	Stop the system from running
Malicious Code	Take control of the system	Change in the system
Jamming Attack	Prevent sensors from detecting. Text follows	Stop the system from running

Table 1. Cyber threats and effect

4.1. Network-Based Intrusion Detection Systems

Network-based attacks are becoming widespread and complex. Therefore, the focus has shifted from operating systems and computers to the network itself. Network-based attack detection is difficult because network inspection generates large amounts of data, and different cases related to a single attack can be seen in different parts of the network. Messages generated during an attack can only be detected as malicious in certain subsections of the network, depending on service configuration and network topology. A single component cannot identify intrusions. There are some requirements for detection (Comert et al., 2018), (Vigna et al., 1998).

- It should create a minimum amount of traffic over the network. Hence, some local processing of incident data is required.
- The number of Network Intrusion Detect Systems it will work with must be scalable.
- Must be able to work with Host-Based IDS.

4.2. Host-Based Intrusion Detection Systems

They run on a single computer on the system computers themselves. They examine data from the network. They provide detection of attacks on systems. There are well-known ways to avoid Network-Based IDSs. Hence, Host-Based-IDS can be used. In intrusion detection, the content should be sent to the

central server where it can be seen clearly and where these avoidance techniques do not work to be processed. On systems, BlueBox is a kind of host-based real-time intrusion detection system and can also be configured to prevent intrusions. Because an attack on a system must gain unintended access to sensitive system resources to be successful, a BlueBox policy defines and enforces rules that control the process's access to system resources, thereby preventing unwanted access. BlueBox captures the resources used in the background. Its rules include:

- Request for access to file system objects,
- Access to the file system,
- Allowed uid and gid entries,
- Use of sent, received, stopped, blocked signals,
- Basic controls for other system resources such as IPC objects and IOCTL calls.

Since system resources must be accessed via system calls, it does not allow access to resources if a system call is not invoked. Some various mechanisms and tools can be used to create and specify rules for a particular program. In order to use these rules and tools, it is necessary to configure new servers. 72 system calls are considered harmless in the system (Chari et al., 2003). Data entries considered harmless by BlueBox are shown in Table 2.

Resources	**Types of access**
File system objects	create, open, read, write, execute, removal, link–to change of access permissions, change of ownership
File systems	mount, unmount, types of mounts
Identities	acquire, release, inherit
Processes (address spaces, signals)	read, write, deliver
CPU cycles, process scheduling priority	raise
System clock	set, read
System/kernel memory	read, write
IPC objects: pipes, semaphores, message queues, shared memory	create, open (attach), read, write
Devices, network	create/attach, open, read, write, io–control, removal, link–to, change of access permissions, change of ownership
Privileges	acquire, release, raise, lower

Table 2. 72 System calls are considered harmless in the host-based detection system.

5. CONCLUSION

Attacks on the smart traffic lights system cause events that endanger human life in traffic. All the lights and signs in the smart traffic lights system can be controlled with the buffer overflow attack. As a result of this happening, people may be misled, and accidents may occur. With a DoS attack, all data in the smart traffic lights system can be temporarily stopped. Stopping the data flow may disable the smart traffic lights system that works depending on the traffic density. Therefore, misdirection for drivers and pedestrians can cause traffic accidents, delays, loss of life, and property. With the jamming attack, the traffic response smart traffic lights system can be temporarily disabled. The system can be controlled as desired with the Malware code. The result of the attacks generally results in loss of life and property. In addition, time is lost. Network-based and host-based scans can be performed to prevent and control attacks. If the attacks are made over the network, the network-based instruction detection system detects them from the network movements. However, if the data has input and movement on the system, the host-based instruction detection system detects it. The system completely blocks detected attacks. In this way, the smart traffic lights system becomes safer. With this study, it is possible to take over the systems from the central direction by using the cyber-attack methods of smart traffic lights. In addition, this study clearly shows that these systems should be protected in layers and that firewalls should be placed between each layer. There are not many studies in this area that cause the lack of new model proposals. Smart transportation systems should be added to the work done in the field of cyber security, and the situation of smart transportation should be studied.

REFERENCES

Asad, B., Saxena, N., & Katos, V. (2021). Analysis of the security and privacy risks and challenges in smart cities' traffic light system, pp. 2–7.

Avcı, İ., Aydın, M. A., Koca, M., 2017. Optik Ağlarda Güvenlik Açıkları ve Çözüm Yöntemleri Hakkında Bir Araştırma Çalışması (IATS'17), pp.395-405, October 19-22, Fırat University, Elazığ, Turkey.

Avcı, İ., Özarpa, C., Aydın, M. A., 2020. A Survey of International Security Standards for Smart Grids, Industrial Control System and Critical Infrastructure, 12th International Exergy, Energy and Environment Symposium (IEEES-12), December 20-24, Doha, Qatar.

Chari, S. N., and Cheng, P. C., 2003."Bluebox: A policy-driven, host-based intrusion detection system," ACM Trans. Inf. Syst. Secure., vol. 6, no. 2, pp. 173–200, DOI: 10.1145/762476.762477.

Cheng, C., & Lee, E. A., 2008. Specification and Formal Verification of Real-Time Systems under Ptolemy II.

Comert, G., Pollard, J., Nicol, D. M., Palani, K., and Vignesh, B., 2018. "Modeling cyber-attacks at intelligent traffic signals," Transp. Res. Rec., vol. 2672, no. 1, pp. 76–89, DOI: 10.1177/0361198118784378.

Hakiri, A., & Berthou, P., (2015). Leveraging SDN for the 5G networks: Trends, prospects, and challenges. arXiv preprint arXiv:1506.02876.

Javaid, U., Siang, A.K., Aman, M.N. and Sikdar, B., 2018. "Mitigating IoT device-based DDoS attacks using blockchain," CRYBLOCK 2018 - Proc. 1st Work. Cryptocurrencies Blockchains Distrib. Syst. Part MobiSys 2018, no. June, pp. 71–76, DOI: 10.1145/3211933.3211946.

Kang, T. U., Song, H. M., Jeong, S., and Kim, H. K., 2018. "Automated Reverse Engineering and Attack for CAN Using OBD-II," IEEE Veh. Technol. Conf., vol. 2018-August, pp. 10–16, DOI: 10.1109/VTCFall.2018.8690781.

Kumar, P. D., Nema, A., and Kumar, R., 2009. "Hybrid analysis of executables to detect security vulnerabilities," Proc. 2nd India Softw. Eng. Conf. ISEC 2009, pp. 141–142, DOI: 10.1145/1506216.1506248.

Mustapa, M. (2007). Smart traffic light.

Morimoto, S., Wang, F., Zhang, R. and Zhu, J., 2018. "Cybersecurity in Autonomous Vehicles," Researchgate.Net, no. May 2017, DOI: 10.13140/RG.2.2.31503.23207.

Nam, T., & Pardo, T. A., 2011. Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, pp. 282–291, ACM.

Özarpa, C., Aydın, M. A., Avcı, İ., 2021. International Security Standards for Critical Oil, Gas, and Electricity Infrastructures in Smart Cities: A Survey Study, Innovations in Smart Cities Applications Volume 4, Chapter 89, Springer.

Sedjelmaci, H., Senouci, S. M., and Ansari, N., 2018. "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," IEEE Trans. Syst. Man, Cybern. Syst., vol. 48, no. 9, pp. 1594–1606, DOI: 10.1109/TSMC.2017.2681698. 8

Tandem Trafik, "Akıllı Trafik Sistemleri," https://www.tandemtrafik.com.tr/tr/akillitrafik-sistemleri/ (1 June 2021)

Vassallo, E. W., and Manaugh, K., 2018. "Spatially clustered autonomous vehicle malware: Producing new urban geographies of inequity," Transp. Res. Rec., vol. 2672, no. 1, pp. 66–75, DOI: 10.1177/0361198118794057.

Vigna, G., and Kemmerer, R. A., 1998. "NetSTAT: A network-based intrusion detection approach," Proc. - Annu. Comput. Secure. Appl. Conf. ACSAC, pp. 25–34, DOI: 10.1109/CSAC.1998.738566.

Zheng, B., Lin, C. W., Shiraishi, S. and Zhu, Q., 2019. "Design and analysis of delay-tolerant intelligent intersection management," ACM Trans. Cyber-Physical Syst., vol. 4, no. 1, pp. 1– 27, DOI: 10.1145/3300184.