Secure Controls for Smart Cities; Applications in Intelligent Transportation Systems and Smart Buildings

Barbara T Hyman, Zahra Alisha, Scott Gordon

International Journal of Science and Engineering Applications
Volume 8–Issue 06,167-171, 2019, ISSN:-2319–7560

Secure Controls for Smart Cities; Applications in Intelligent Transportation Systems and Smart Buildings

Barbara T. Hyman
California State University
Sacramento, CA 95819

Zahra Alisha
California State University
Sacramento, CA 95819

Scott Gordon
California State University
Sacramento, CA 95819

Abstract: Internet of Things (IoT) is an emerging concept in smart infrastructures describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. IoT is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures by enhancing their quality of service provisioning.
Smart infrastructure, enabled by technologies like IoT, offer numerous of advantages bringing serious cost savings and efficiencies. These kinds of data-driven environments, fueled by connected devices and network connectivity, become a new attack surface for cyber threats. Cyber security approaches develop guidance to secure IoT and Smart Infrastructures from cyber threats, by highlighting good security practices and proposing recommendations to operators, manufacturers and decision makers. In this paper, cyber security approaches are analyzed in a smart city infrastructure.

Keywords: Internet of things; Cyber security; Smart transportation; Smart city.

1. INTRODUCTION

Nowadays buildings are not only walls, floors and ceilings. By applying artificial intelligence (AI), internet of things (IOT), and in general smart technologies, building systems autonomously collect all the information from IoT devices, occupant behavior, and environment to learn from the data, analyze it, optimize the performance and eventually improve the building efficiency. As a matter of fact, by applying innovative IOT and AI embedded platforms in today smart buildings, the occupants satisfaction is improved significantly. Moreover, the new smart buildings make it possible to radically reduce costs through management, automation, and optimization of operations in a smart environment [1-7].

A comprehensive building management system leverages all aspects of building facilities; e.g., [3], [4]. In [3], the developed smart building with IOT solutions allows for monitoring all the living conditions; e.g., temperature, humidity, energy allocation, movements, etc. In [4], all the aspects related to the heating, ventilation, and cooling (HVAC) system in a smart building are managed and optimized. All the data related to the HVAC system of each zone is used to trigger the distributed control algorithms to not only detect but also predict and respond to anomalies [4]. In other words, the smart building technologies are employed to identify possible root causes, so actions can be prioritized, assigned, monetized and prevented. Recommendations that appear on dashboards or adjustments is transmitted directly to the IoT device for quick and efficient actions. Introducing smart automation infrastructures in smart buildings increases the residents convenience and reduces the labor operational costs, however, these new facilities dramatically increases the level of potential vulnerability in the smart infrastructure. Examples of these vulnerabilities are disgruntled employees, cyber criminals, cyber attackers, etc. The problem is that any control system can be attacked internally, therefore there is a need for more efficient protection in a smart environment; e.g., smart transportation system, smart building.

In this paper, we have considered different vulnerability cases in controls of smart transportation systems and smart buildings, and we have discussed and introduced some trustworthy and safe control frameworks for these environments.

The rest of the paper is organized as follows. Section 2 presents the smart building technologies and challenges. Section 3 explains the smart transportation systems technologies and challenges. The next section introduces the failsafe SCADA networks. Sections 5, 6, 7, and 8 present the forensics, engineering, monitoring, and vulnerability management in the smart city environment. Finally, section 9 provides the conclusions and the future research.

2. SMART BUILDING AND CHALLENGES

In a smart building, after the equipment information is collected through sensors and meters, a library of benchmark data is applied, analytics are performed and potential actions toward performance improvement are identified [3]. To automate insights into actions as they optimize assets with IoT, we can utilize the predictive analytics to artificial intelligence or learning systems [4], [5]. By taking advantage of predictive algorithms, building owners can significantly cut energy consumption and achieve ambitious cost-saving targets. For example, by combining data for heating and cooling with weather forecasts, an HVAC system can deliver more efficient heating and cooling; see [4] for more information. Thus, by combining the cognitive analytics and sensors in the existing building systems, we can significantly improve occupant experience. The buildings will be flexible, adaptable and able to predict occupant needs [4]. The features in the fig. 1 can be considered in a smart building or a smart workplace.

- Energy costs and demands for smart building are on the rise.
- Companies are facing aggressive energy reduction targets.
- Increasing IOT adoption is leading to data overload.
- High pressure to address the environmental concerns.

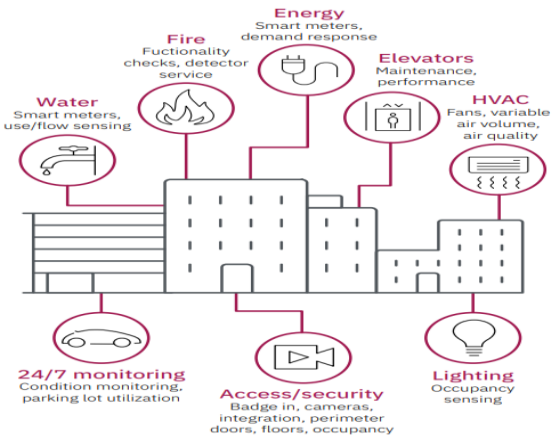

Fig. 1: Smart features in a smart building

3. SMART TRANSPORTATION SYSTEM AIMS AND CHALLENGES

All the components such as automotive, aviation, and rail systems could be considered as the foundation of transportation systems. Also different modes of transportation from land, air to water can be considered in a transportation system. Roads, bridges, parking places, kinds of stations, airports, and shipyards provide the immobilized support and sustenance to all kinds of motions. The interactions between the transportation system components also construct a partition of these systems. Video detectors, microwave detectors, radar detectors, and magneto detectors cause the monitor, control, and communication to happen within the transportation systems. Different sensors are employed in roads or bridges to improve the transportation performance. In a smart transportation infrastructures three main parts exist to provide controls, communication, and computation; the on-board units, the roadside units, and the transportation control unit. Here we have explained each of these components.

- onboard units are the devices/equipment that are installed in the vehicles. They collect the information in the vehicle and process the stored data in the unit's memory.

- The roadside units are the embedded devices along the road to increase the overall coverage of a vehicular system. The vehicles in the coverage area of the roadside units receive messages from them. These units are installed to enhance the propagation delay of messages between disconnected vehicles and eventually increase the transportation network performance.

- The transportation control units are the supporting systems for the two other mentioned units (on-board units and roadside units). The generated data transferred over these control units. These control units can provide optimal decisions and apply the optimal strategies regardless of the time, data, and resources. Fig. 2 shows the relations between the on-board, roadside and control units in a smart transportation network.

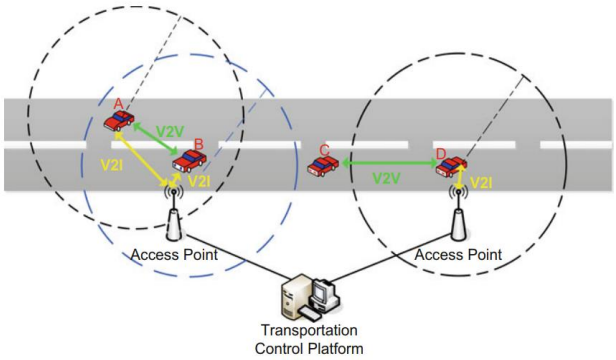

Fig. 2: Three units relation in a smart transportation network

Since the computational overhead and complications is fairly high in data analytics and controls of intelligent transportation systems, the centralized approaches is not enough in designing Fig. 2: Three units relation in a smart transportation network a management system for them. Distributed and decentralized control designs come to play for the mentioned reasons. Wireless communication networks are being commonly used in the smart transportation systems. WAVE/802.11p and ZipBee/802.15.4 are two very common communication protocols for data collection and transportation because of their improved abilities of data exchange among the vehicles and between the vehicles and the roadside infrastructures [6], [7]. Wireless sensor networks (WSNs) in also play a very important but not conspicuous role. WSNs consist of spatially distributed autonomous sensors to monitor physical conditions such as temperature, sound, pressure, and the like, and to transfer sensed data through wireless networks to sink nodes then return to the control unit. The communications in s mart transportation system are processed as in a WSN, but should concern mobility. Traditionally, there have been two types of transportation systems communications for decades: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. The third type of communication is built upon V2I and V2V based on long-distance wireless communication with the support of vehicle manufacturers or mobile service carriers (ATT, T-Mobile, Verizon, etc.). The third type of communication is known as the device-to-device (D2D) communication. Different from V2V and V2I, D2D is a multi-dimension channel that not only provides simple information exchange but also supports the interaction of images, sounds, and GPS location information. Furthermore, with the assistance of smartphone, many location-based services also benefit from the third type of communication and produce many applications (Google Map, Apple Map, etc.). Fig. 3 shows the three common types of communications in a smart transportation system.

4. FAILSAFE SCADA NETWORK

SCADA networks are commonly useful for building industrial control systems, as a prominent infrastructure. There are various vulnerabilities exist in wired or wireless communication networks of SCADAs. As a matter of fact, the

communication networks can be intruded to terminate or misroute the control commands. Fig. 4 shows an SCADA networks with its local area network (LAN) and wide area network (WAN) communications. For having more safety, there can be additional layers of security in conveying commands to vital switches. For instance, a backup system can be provided in case that the system providing the confirming codes break down.

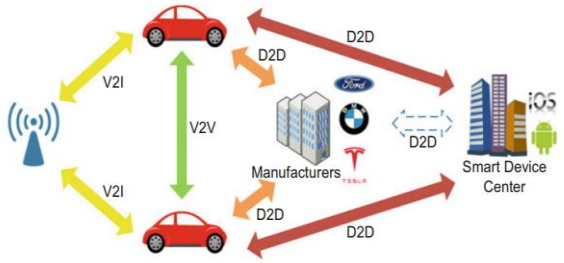

Fig. 3: Three units relation in a smart transportation network

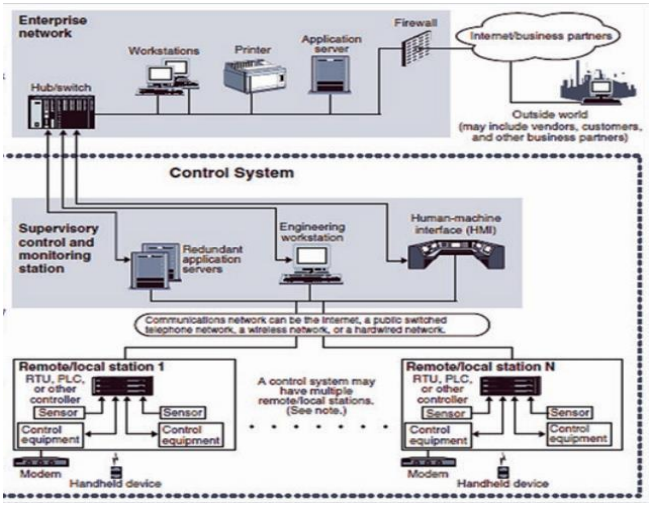

Fig. 4: Supervisory control and data acquisition (SCADA) components and communication networks

Predicting all the possible failures or malfunctions in the network equipment or communications due to the attacks or actuators faults is complicated, costly, and time consuming. This is where the human-machine interface comes to play. The human-machine interface display provides necessary information to the operators of SCADAs. HMI can send alerts to human operators when needed, or it can indicate errors. The return signals alert the malfunctions such as pipeline leaks, pumping station equipment failures, and sewage pipe blockage. The most important error signals that can be sent to the operators is the signals showing the cyber-attacks to the SCADA software. Although the artificial intelligent (AI) algorithms can be used to manage and monitor most of the SCADA alerts/errors, it is very important to quickly detect the anomalies and to quickly correct them. Therefore, it is necessary to always have human operators in the loop, along with the embedded AI algorithms. To improve the network safety in a SCADA system, the backup communications from and to the HMI are provided. There are various types of cyber attacks in SCADA systems; database attacks, communication attacks, common protocols vulnerability, network holes, and field devices attacks. The centralized architecture is not efficient in case of cyber attacks in the SCADAs, since an anomaly may cause the vital infrastructure to shut down immediately. Thus, the decentralized structure may improve the system performance by allowing the isolation of the attacked subsystems or failed subsystems. The protective measures can be improved by considering the system operators information. The following protective measure are recommended in this paper:

- Apply technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
- Evaluate the security level of all the remote sites connected to the SCADA network.
- Establish teams to test and evaluate attack scenarios on the SCADA.
- Define and specify the cyber security responsibilities of managers, system administrators and users.
- Provide a documents about the network architecture and systems that serve critical functions or contain sensitive information; i.e, systems that require additional levels of protection.
- Construct a rigorous, ongoing risk management process.
- Build a network protection strategy based on the defense in-depth.
- Identify cyber security requirements with specific details.
- Establish effective configuration management processes.
- Conduct routine self-assessments.
- Establish system backups and disaster recovery plans.
- Establish expectations for cybersecurity performance and hold individuals accountable for their performance.
- Construct policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

- Implement internal and external intrusion detection systems and establish 24-hours-a-day incident monitoring.
- Establish strong controls over any medium that is used as a backdoor into the SCADA network.
- Implement the security features provided by device and system vendors.
- Do not rely on proprietary protocols to protect your system.
- Harden SCADA networks by removing or disabling unnecessary services.
- Evaluate and strengthen the security of any remaining connections to the SCADA network.
- Disconnect unnecessary connections to the SCADA network.
- Identify all connections to the SCADA network. To protect the control system in a SCADA system, four critical processes need to be done; digital forensics, engineering and architecture, operation monitoring, and vulnerability management. Fig. 5 shows the relationship between these four required processes to attain protection in the SCADA system.

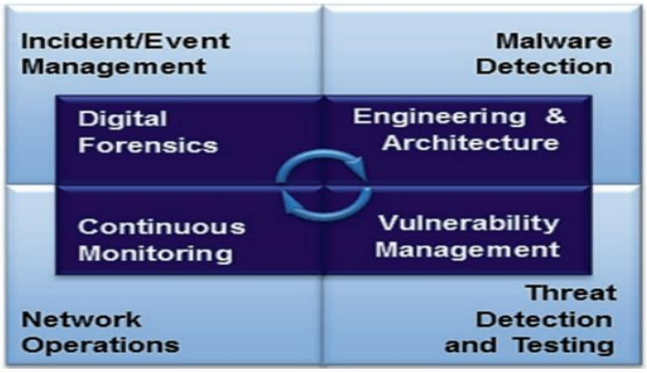

Fig. 5: Four required processes to attain protection in SCADAs

5. DIGITAL FORENSICS

The digital forensics process consists of three steps: acquisition or imaging of exhibits, analysis, and reporting. Ideally acquisition involves capturing an image of the computer's volatile memory and creating an exact forensic duplicate of the media, often using a write blocking device to prevent modification of the original. However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device. Both acquired image (or logical copy) and original media/data are hashed (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate. During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools. The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices). The evidence recovered is analyzed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialized staff. When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

6. ENGINEERING AND ARCHITECTURE

All the industrial infrastructures must be designed to be robust against cyber attacks databases attacks, and IT networks or communications systems attacks, either directly in real time or a later time. The hardware and software must not only be designed to protect against malware attacks, but it also must be designed with enough flexibility and modularity so that the control software and hardware can be upgraded and improved over time. The design should also be flexible so that any malware attack can be compartmentalized and contained or isolated until repairs are made and normal service is restored. Possible design elements include secret authentication features that are isolated from most system operators and are based on key functions requiring approvals from top management. There also could be delays in some execution of control commands with alerts to high level supervisors before implementation unless verified by an additional security code. Such authentication systems would be most protective against cyber criminal or techno-terrorist attack if they can be executive from a more location. The trouble with such authentication code verification can is if there is a communications or component failure or a supervisor who is suddenly unavailable, blocking a critical valid control command. Such systems require extra redundancy, and no system can ever be failsafe despite what design engineers might claim [7].

7. OPERATION MONITORING

Continuous monitoring is vital to successful network operations of any type of industrial or urban infrastructure, regardless whether this is for transportation, energy systems of all types, communications or IT systems, water and sewage systems, etc [8-10]. SCADA systems not only exercise supervisory control but also provide vital data acquisition to ensure that network operations are as they should be. Continuous monitoring must not only examine incoming data to ensure that networks are performing normally but are also built to detect spurious data providing incorrect information. Thus continuous monitoring might include random coded signals that require a proper authentication response to verify that it is live data coming through rather than faked readout such as simple repeats of previous data reports. In short, continuous monitoring at the human-machine Interface must

involve more than passively awaiting problem alerts. Some form of diagnostic authentication system needs to be a part of the continuous monitoring systems of the future.

8. VULNERABILITY MANAGEMENT

Threat detection and testing of end to end systems is vital to the safe and reliable operation of a smart industrial control system. Vulnerability management includes not only executing a successful response to block an attempted intrusion but is an active process of continuous monitoring and testing to make sure that operations are indeed normal and that incoming data is not being synthesized by a cyber-attacker. This verification process either involves active testing or authentication of incoming data via coded messaging, algorithms that detect abnormal data, or other testing processes. It is also important to study reports of intrusions from other operational networks and to consider case study reports concerning lessons learned from cyber attacks that have utilized new and improved techniques, software or hardware to stop cyber-attacks against parallel systems.

9. CONCLUSIONS

There are many different approaches to prevent cyber attacks. Access codes, dual authentication systems, smart algorithms that do not allow dangerous activities with regard to dams, bridges, traffic signals, power plants, energy grids and more without the highest level of authorization and multiple authentication codes can be used to prevent abuses of smart infrastructure. Defensive systems can only go so far to protect digital networks and modern urban infrastructure. At some point proactive cyber security systems will need to find the cyber criminals and techno-terrorist attackers and bring them to justice. Changes to the Internet architecture and controls on the Internet of Things (IoT) as it becomes the Internet of Everything (IoE) may be necessary. Likewise efforts to probe the dark web and bring some form of controls to electronic monetary systems such as bit coin may also become necessary. This is no simple or easy task. Personal freedom and liberty from government surveillance are keys to democratic processes. It may well be that clever technological solutions may be found to the problems that come with more and more automation in 21st century society.

10. REFERENCES

[1] Pinson L. and Jinnett J. Anatomy of a Business Plan : A Step-bystep Guide to Start Smart, Building the Business and Securing Your Company's Future. 3rd ed. Chicago: Upstart Pub., 1996.

[2] Jadhav N. Y. Green and Smart Buildings : Advanced Technology Options. Green Energy and Technology. Singapore: Springer, 2016.

[3] Eini R., Linkous L., Zohrabi N., Abdelwahed S., "A Testbed for a Smart Building: Design and Implementation," Proceedings of the 4th International Workshop on Science of Smart City Operations and Platforms Engineering, April 15-18, Montreal, QC, Canada, 2019. DOI: 10.1145/3313237.3313296

[4] Eini R. and Abdelwahed S., "Distributed Model Predictive Control Based on Goal Coordination for Multi-Zone Building Temperature," 2019 IEEE Green Technologies Conference (GreenTech), Lafayette, LA, 2019.

[5] Eini R., and Abdelwahed S., "Rotational Inverted Pendulum Controller Design using Indirect Adaptive Fuzzy Model Predictive Control," *International Conference on Fuzzy Systems 2019,* New Orleans, USA, June 2019.

[6] Eini R. and Abdelwahed S., "Distributed Model Predictive Control for Intelligent Traffic System, In Proceedings of the 15th IEEE International Conference on Green Computing and Communications (GreenCom-2019), Atlanta, USA, July 2019.

[7] Kacprzyk J., Alam M., Ferreira J., and Fonseca J. Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety. 1st Ed. 2016 ed. Vol. 52. Studies in Systems, Decision and Control. Cham: Springer International Publishing, 2016.

[8] Proper A. T. Systems, and United States. Intelligent Transportation Systems Benefits: 1999 Update. U. S. Dept. of Transportation, 1999.

[9] Picone M., Stefano B., Michele A., Francesco Z., and Gianluigi F. Advanced Technologies for Intelligent Transportation Systems. Vol. 139. Intelligent Systems Reference Library. Cham: Springer International Publishing, 2015.

[10] Arab N., and Kamrani A. K. Intelligent Transportation and Evacuation Planning A Modeling-Based Approach. 2012.