IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 7, 2019, accepted May 25, 2019, date of publication June 4, 2019, date of current version July 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920763

Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities

XING LIU, CHENG QIAN, WILLIAM GRANT HATCHER, HANSONG XU, WEIXIAN LIAO, AND WEI YU

Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA

Corresponding authors: Xing Liu (xliu10@students.towson.edu), Cheng Qian (cqian1@students.towson.edu), William Grant Hatcher (whatch2@students.towson.edu), Hansong Xu (hxu2@students.towson.edu), and Wei Yu (wyu@towson.edu)

This work was supported by the U.S. National Science Foundation (NSF) under Grant CNS 1350145.

ABSTRACT The widespread adoption of the Internet of Things (IoT) technologies has drastically increased the breadth and depth of attack surfaces in networked systems, providing new mechanisms for the intrusion. In the context of smart-world critical infrastructures and cyber-physical systems, the rapid adoption of the IoT systems and infrastructures without thorough consideration for the risks and vulnerabilities has the potential for catastrophic damage to the privacy, safety, and security of individuals and corporations. While the IoT systems have the potential to increase productivity, accountability, traceability, and efficiency, their potential weaknesses are also more abundant. In this paper, we provide critical consideration of the security of the IoT systems as applied to smart-world critical infrastructures. Particularly, we carry out a detailed assessment of vulnerabilities in IoT-based critical infrastructures from the perspectives of applications, networking, operating systems, software, firmware, and hardware. In addition, we highlight the three key critical infrastructure IoT-based cyber-physical systems, namely the smart transportation, smart manufacturing, and smart grid. Moreover, we provide a broad collection of attack examples upon each of the key applications. Furthermore, we introduce a case study, in which we assess the impacts of potential attacks on critical IoT-based systems, using the smart transportation system as an example. Finally, we provide a set of best practices and address the necessary steps to enact countermeasures for any generic IoT-based critical infrastructure system.

INDEX TERMS Cyber-physical systems, Internet of Things, security, critical infrastructure, case study, computing infrastructure.

I. INTRODUCTION

Advances in information communication technologies have given rise to the Internet of Things (IoT), which will play an increasingly important role in our daily lives [1]–[3]. In IoT, the massive number of deployed IoT devices (sensors, actuators, etc.) will be connected to collect data related to objects in critical infrastructures, including city and government, industrial manufacturing, energy, transportation, healthcare, and public safety infrastructures, among others, supporting numerous smart-world systems. The examples of such systems are smart manufacturing, smart cities, smart grid, smart transportation, smart home, and smart health systems, to name a few [4]–[11].

The associate editor coordinating the review of this manuscript and approving it for publication was Jinsong Wu.

With the rapid development of IoT that can be used to support smart-world critical infrastructure systems, innumerable sensors and actuators, both of which are called IoT devices in general in this paper, are being deployed so that monitoring and control capacities across a variety of CPS/IoT domains can be enabled. Given their increasing popularity and the novel applications they can enable, the volume of IoT devices deployed and in use is expected to reach approximately 31 billion by the year 2020 [12], and will only continue increase in number. Nonetheless, cyber-threats could pose serious security risks to IoT devices, disrupting the effectiveness of the systems supported by IoT devices. Smart devices have repeatedly been demonstrated to be vulnerable and were easily employed in a recent attack on October 21, 2016. This attack caused numerous popular websites becoming unreachable [13]. This attack was raised by a number of unknowingly

compromised, mass-produced smart consumer devices such as webcams and related products. Other recently exposed vulnerabilities in critical smart systems include implantable cardiac devices susceptible to remote reprogramming and rapid battery depletion [14], widespread ''mission-critical'' vulnerabilities in smart weapons systems for the US military [15], [16], and ransomware attacks that disrupted 34 % of England's Nation Health Service [17]. As an emerging threat, IoT security and susceptibility to intrusion reaches all aspects of society, implicating all domains of cyber-physical systems (CPS) and smart-world systems. The typical examples of such systems include the smart home, smart grid, smart transportation, smart manufacturing, smart healthcare, and others.

For instance, the smart manufacturing system, that is, IoT applied to industrial systems to greatly improve productivity, and operational and resource efficiencies [6], [18], has seen its share of cyber-attacks [19]–[24], which have typically targeted the disruption of regular operation, such as the Stuxnet worm for gaining control of programmable logic controllers (PLCs) [25] and malware attacks on HVAC systems [26]. The smart transportation system that interconnects vehicles, infrastructure (e.g., road side units (RSUs)), people, and the Internet [27]–[29] has been shown be vulnerable, allowing for the full remote control of the vehicle, as well as vehicle impersonation and the sending of false information to RSUs, nearby vehicles, etc. via Sybil attacks [30]–[32]. The smart grid, which integrates massively numerous electrical microgrids via extensive two-way communications between power suppliers and consumers relies heavily on the availability of measurement data to conduct accurate and real-time state estimation and efficient system operations. Nonetheless, effective and efficient operations of the smart grid have shown vulnerabilities to the disturbance of state estimation via data integrity attacks, false data injection attacks, and so on [5], [9], [33]–[40]. The smart healthcare system, which aims to improve patient care through a growing number of sensors that assess patient health conditions, must adhere to strict oversight and regulation requirements for data confidentiality [41]–[43]. Yet, despite these regulations, a number of smart healthcare systems have been subverted, including by viruses like WannaCry, Medjack [44] and SamSam that disrupted hospitals as recently as February 2018, and via potentially life-threatening vulnerabilities such as those found in the Carelink 2090 pacemaker.

While a number of research efforts have been conducted toward enhancing the security of critical infrastructure systems, the majority of existing research has focused only on the vulnerabilities of sensing and measurements, such as data integrity attacks against measurement devices, and a comprehensive investigation into the impacts of vulnerable actuators on the critical infrastructure systems themselves has not been explored. For instance, intrusions of IoT devices have increased dramatically due to IoT devices being much easier to compromise than conventional devices, owing to their limited resources, lack of security software, multitude of network interfaces (Ethernet, Bluetooth, WiFi, ZigBee, etc.), and human factors like not changing default passwords. For these reasons, vulnerabilities abound, and the sheer volume of devices make distributed denial-of-service (DDoS) attacks the primary use for those subverted. Thus, there is an imminent need for a systematic exploration of the space of attacks against IoT systems (smart plugs, smart bulbs, smart manufacturing controllers, etc.) in critical smart infrastructure systems, investigation into the risks of those attacks, and development of countermeasures for their mitigation.

To fulfill this need, and to assess all aspects of IoT-based cyber threats thoroughly and completely, we investigate vulnerabilities of IoT systems from the perspectives of the network layer, operating system, software, firmware, and hardware. Vulnerabilities in the network layer can be allocated into six attack surfaces, which are the device networking service, device web interface, mobile application, cloud interface, privacy, and network traffic. For example, adversaries can attack the device network service through vulnerabilities that include unencrypted services, poorly implemented encryption, and denial of service. Vulnerabilities in the operating system can be grouped via administrative interface, update mechanism, and privacy. Likewise, software vulnerabilities can be identified by third-party backend application programming interfaces (APIs) and vendor backend APIs. The device firmware and update mechanism are categories of firmware vulnerabilities. Finally, device hardware (sensors) and physical device interfaces are categories of the hardware vulnerabilities.

To investigate cyber-attacks in IoT systems, we first propose a three-layer architecture (i.e., service layer, operation layer, and management layer) to study the key IoT systems, such as smart transportation, smart manufacturing, and smart grid. The service layer consists of various services, such as the mobility management service and the driver assistant service in smart transportation, the raw material supplement service and the smart logistics service in smart manufacturing, and the distributed energy integration and storage service in smart grid. The operation layer ensures safe and efficient operation on diverse systems, including route management operation and turn-by-turn navigation operation in smart transportation, function and process automation operation in smart manufacturing, and demand response and energy distribution in smart grid. The management of IoT systems ranges from information management to emergency management, which ensures key modules in IoT are functioning properly, such as information, maintenance, facility management, among others.

From the perspective of the three-layer architecture outlined, we next consider cyber-attacks on several representative smart-world systems, including smart transportation, smart manufacturing, and smart grid, detailing the attack targets, definitions, examples, and impacts. Then, we study the impacts of both individual small-scale and combinatorial large-scale attacks in disrupting IoT system service, operation and management in the cases of smart transportation, smart

manufacturing, and smart grid. Moreover, we conduct a case study on the impacts of cyber-attacks on smart transportation via extensive experimentation. In particular, we study the least-effort attack (achieving target objectives, such as disruption of a vehicular network and traffic, with minimum attack cost) on smart transportation. The results demonstrate that a combined attack on both vehicles (signal transmission) and traffic lights (frequency) can obtain maximum damage (i.e., denial of service and traffic congestion) via manipulating the least number of vehicles or traffic lights.

Finally, we propose countermeasures to protect IoT systems from cyber-attacks via a generalized three-phase framework. In the first phase, we shall investigate the risks of cyber-attacks on diverse IoT systems, considering system vulnerabilities, impacts of vulnerabilities on key functions, and optimal attack strategies from the perspective of an adversary. In the second phase, we shall investigate defensive schemes based on the design of resilient IoT-based systems, optimal IoT-based system configurations, effective cyber-attack detection, and timely cyber-attacks response. In the third phase, we shall leverage an integrated experimentation platforms to capture the dynamics of IoT systems and evaluate the performance of the proposed defensive schemes, utilizing tools such as the Fenix framework for Network Co-Simulation (FNCS) in simulating the smart grid system [11], OMNET++, SUMO, and Veins for simulating the smart transportation system [45], and the wireless cyber-physical simulator (WCPS) for simulating the smart manufacturing system [46].

The remainder of this paper is as follows. In Section II, we provide categorical study of IoT vulnerabilities. In Section III, we describe key applications in IoT from the perspective of our three-layer architecture. In Section IV, we present a study of cyber-attacks on IoT applications, outlining attack targets, examples, and impacts. In Section V, we present our own case study investigating least effort cyber-attacks on the smart transportation system. In Section VI, we discuss security countermeasures in IoT from the perspectives of risk assessment, defensive schemes, and testing and evaluation platforms. Finally, in Section VII, we provide concluding remarks.

II. IOT VULNERABILITIES

In this section, we categorically investigate vulnerabilities in IoT. To achieve a clear picture of the IoT vulnerability landscape [47], we subdivide IoT systems based on a traditional layered or tiered structure. We then identify the IoT attack surfaces and classifying the vulnerabilities.

In considering vulnerabilities in IoT, we first consider a basic layered computer system structure to divide the IoT system. In this case, we have identified five primary layers in the IoT system: the network layer, the operating system, software, firmware, and hardware. Fig. 1 shows a breakdown of the layered structure, as well as the subdivisions of each layer that make up our entire classification scheme. We now present each layer in detail, along with the attack surfaces and vulnerabilities.

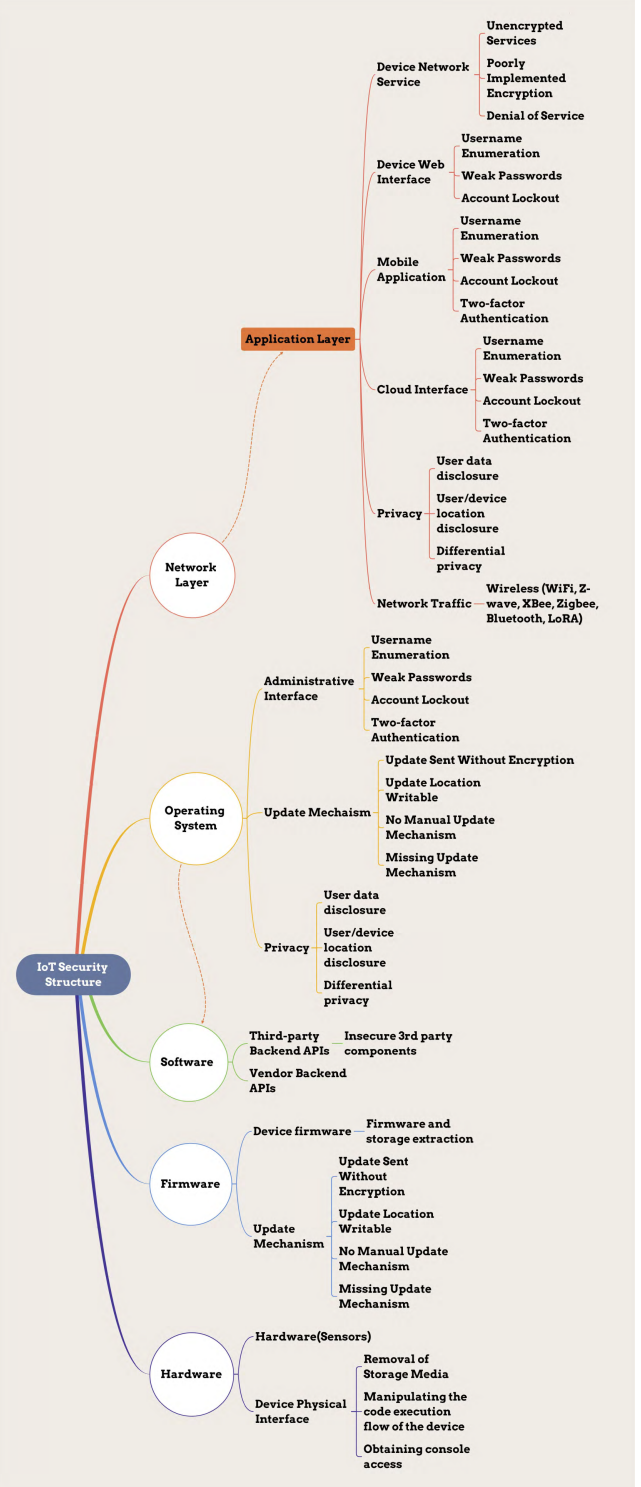

FIGURE 1. IoT vulnerability structure.

A. NETWORK LAYER

The network layer is where the IoT devices transfer data. This data transfer requires the support of various protocols, such as TCP/IP protocol. Based on the Open Systems

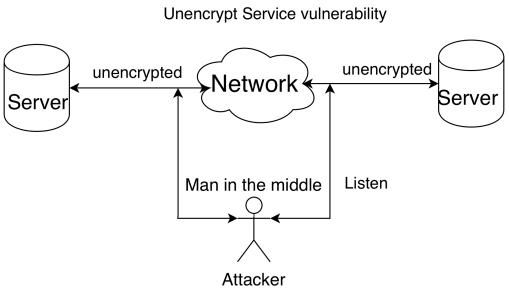

FIGURE 2. Unencrypted Service vulnerability.

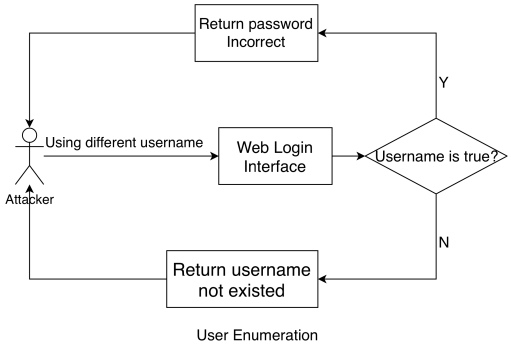

FIGURE 3. User enumeration.

Interconnection (OSI) network model, we consider attack surfaces to reside primarily in the network application layer. In the network application layer, there exist six attack surfaces. These attack surfaces are the device network service, device web interface, mobile application, cloud interface, privacy and network traffic.

1) DEVICE NETWORKING SERVICE

The device network service attack surface is where all communication services are running. This attack surface has three kinds of vulnerabilities, which are (i) *Unencrypted Service.* The unencrypted service vulnerability is one in which data is transferred in clear text, readable by anyone that can receive the data. In this case, an adversary can listen to the communication via Man-In-The-Middle (MITM) [48], [49] attack, as demonstrated in Fig. 2. (ii) *Poorly Implemented Encryption.* It is a vulnerability in which the encryption implemented in a system is either poorly configured or the is out of date (Like the SSLv2/v3) and therefore ineffective. Just as in the prior vulnerability, the MITM attack can be used here as well. (iii) *Denial of Service.* It controls millions of compromised devices to send requests to one victim simultaneously over some duration of time [50]. An example is the Memcached Amplification Attack [51] that occurred on Feb 28, 2018, which is called an amplification attack because it exploits a disparity in bandwidth consumption between an adversary and the targeted web resources. This attack only requires a small query and can instigate huge attack traffic. Additionally, DRDoS attacks on IoT devices have demonstrated methods to affect IoT devices without compromising them [52].

2) DEVICE WEB INTERFACE, MOBILE APPLICATION, AND CLOUD INTERFACE

Because these three attack surfaces have the same four kinds of vulnerabilities, we illustrate these vulnerabilities only once in the following to reduce repetition. The device web interface one is usually displayed as a login page. The mobile application is the most common, otherwise denoted as an app, with examples like Facebook, Twitter and many others. These applications also have login functions or pages equivalent to those of the device web interface attack surface. The cloud interface is relevant to cloud computing.

We now illustrate some threats against those three attack surfaces as follows: (i) *Username Enumeration.* The username enumeration vulnerability is a kind of brute force attack in which the adversary will attempt login using several different usernames from a dictionary. If one of the usernames matches the username in the website, other services' databases will return information indicating ''password incorrect''. Then, the adversary knows the username matched, and he or she will only need to guess the correct password to compromise the IoT system. Another case study on general IoT vulnerabilities has illustrated the damage of such attacks [53]. (ii) *Weak Password.* It is generally self-explanatory, where users set very simple or common passwords, often only comprised of numbers or characters. For example, '1111111', 'password', and 'birthdaycake' are typical weak passwords. Weak password like the examples make the compromise of victim devices quite simple with brute force attacks. Several articles mentioned these risks as they pertain to IoT devices [53], [54]. (iii) *Account Lockout.* The account lockout vulnerability uses a brute force attack to trigger security mechanisms that include lockout (temporarily disabled login) of normal users from their accounts, denying them access [55]. Additionally, cases where systems do not have account lockout can be dangerous to IoT devices [53], revealing to an adversary the potential to brute force attack the login and password indefinitely. (iv) *Two-factor Authentication.* The two-factor authentication [56] vulnerability is one, in which the two-factor authorization process is compromised by an adversary to gain entry. The adversary could use a company's credentials or build a low-cost honey-pot-like server to intercept the two-factor data transmissions.

3) PRIVACY

The privacy attack surface gained significant attention recently, especially in the context of IoT devices. For instance, smart home devices like smart IP cameras, smart IR motion sensors, and Artificial Intelligence (AI) speakers, sometimes called all-weather monitor sensors or smart IoT devices, may have access to significant amounts of personal data through various user accounts, as well as real-time spatial or positional information. If these devices are compromised, the volume of private information revealed will be quite damaging.

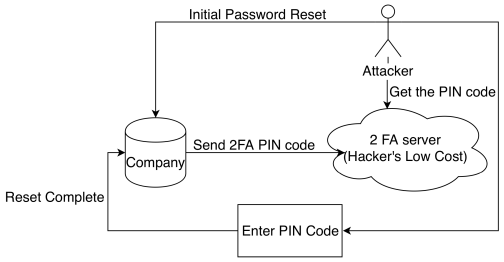

FIGURE 4. 2FA attack.

On this attack surface, we define the following kinds of vulnerabilities: (i) *Username Disclosure.* The username disclosure vulnerability involves an adversary retrieving the username information of the user. With this information, the adversary can then apply the password dictionary in a brute-force attack to guess the password and compromise the system. This has been demonstrated in a real-world case of IP camera ID leakage [57]. (ii) *User/Device Location Disclosure.* This kind of vulnerability implicates very sensitive private information. If the device location disclosed, an adversary could launch an attack with minimal resources deployed to a localized target area, or could implement a more damaging attack using knowledge of the target's location and surroundings, such as affecting the power grid or inducing traffic congestion. The risk of location disclosure in IoT devices has been well illustrated, and the introduction of dynamic location agents and location obfuscation mechanisms have been proposed to mitigate it [58]. Differential privacy is a statistical mechanism that attempts to maximize query accuracy and minimize privacy impact on users by quantifying privacy loss and introducing randomness to thwart message reconstruction. Examples using differential privacy have been shown to keep the output of IoT databases safe [59].

4) NETWORK TRAFFIC

The network traffic attack surface includes the vulnerability of many communication protocols, such as the WiFi, Zigbee, Z-wave and so on. Recent attack examples include the recent Z-wave downgrade attack [60], in which the adversary exploited a vulnerability to downgrade the device security level from $S2$ to S_0. The vulnerability towards WiFi network encryption method (WPA2) is a kind of key reinstallation attack. It has an impact on every device using wireless network hardware. The encrypted WiFi network uses the four-way handshake and this attack can trick a victim to reinstall an already-in-use key. This kind of attack can also hijack the TCP streams and add malicious content to them [61]. For the Bluetooth aspect, a cryptographic bug detected on July 24, 2018 and tracked as CVE-2018-5383. This vulnerability can affect Apple, Broadcom, Intel, Qualcomm, and some headset devices. This kind of attack takes place when two devices are do the paring. Since some devices do not support validating the cryptographic key exchange so that the adversary can install a fake key to obtain the session key to listen the communication [62]. For the ZigBee part, the communication between two ZigBee devices sometimes use the default key in Aug. 2018. It enables the adversaries to establish an MITM attack [63].

B. OPERATING SYSTEM

The operating system is the most important software in any multipurpose computing device, as it can make full use of the hardware resources and provide some common and useful services to user applications. On the operating system layer, we consider the following attack surfaces.

1) ADMINISTRATIVE INTERFACE

This attack surface implicates the operating system login and authorization processes [64]. This includes username enumeration, weak password, and account lockout vulnerabilities. The detailed descriptions of these vulnerabilities can be found in the Section II-A.2 of the network layer.

2) UPDATE MECHANISM

It is a critically important part of the operating system for resolving the known vulnerabilities, updating to the newest functionality, etc. Nonetheless, if the upgrade file is modified, it becomes easy for an adversary to change vital parts of the system and gain unintended access to the device. This attack surface has four kinds of vulnerabilities: (i) *Update Transmission Without Encryption.* When an update file is transmitted to clients without encryption, like TLS v1.2 [65], the update mechanism becomes an attack surface. The update file sent in clear text can easily be modified by an adversary to compromise system integrity [66], either by blocking and replacing the file in transit or by substituting the modified update file to unsuspecting hosts from the start. (ii) *Update Location Writable.* The update location writable vulnerability occurs when the update file stored in a server, ready to be deployed, can be modified by firmware before distribution to the users. This has the same result as the update sent without encryption [66]. (iii) *No Manual Update Mechanism.* When no manual update mechanism exists, the client cannot verify and install updates offline, only receiving the update when the server pushes an update package to all users. An adversary can thus launch an attack before the server delivers a new update to clients if the old version has some vulnerability [47]. (iv) *Missing Update Mechanism.* When no update mechanism exists, an adversary can use any existing vulnerability to compromise the whole system, because no patch can be applied to protect against known vulnerabilities [47].

3) PRIVACY

The privacy attack surface has the similar three vulnerabilities as mentioned in Section 2.1.3 of the network layer. This attack surface is similarly important in the operating system layer, and has been shown to be of particular importance in IoT devices [67].

C. SOFTWARE

In the software layer, we consider programs and applications designed for user and automated machine tasks, interfacing, and interaction. As a primary component of software

systems, Application Programming Interfaces (APIs) specify protocols, tools, data structures and communication between multiple subcomponents and subroutines of complex software systems to obfuscate underlying operation and allow for easy interfacing between components. These APIs are a critical component in the software layer and the OS, dividing complex systems into small manageable parts, improving cohesion and reliability between units to improve the system's maintainability and extendibility. In this layer, there are two primary attack surfaces: third-party backend APIs and vendor backend APIs.

1) THIRD-PARTY BACKEND APIS

Third-party backend APIs are used for application software running on operating systems, such as the Google Maps API. In this case, if the API is out of date, an adversary could gain unintended application access or data, such as the location in the Google Maps case. On this attack surface, the vulnerability is the insecure third-party components. Cases of third-party components being insecure include out-of-date or unpatched software, such as old versions of BusyBox, SSH, and so on. Old software has a higher likelihood of vulnerabilities and are typically easier to compromise [68].

2) VENDOR BACKEND APIS

Unlike third-party APIs, vendor APIs provide software interfaces to get access to hardware. For example, hardware maintenance software uses vendor backend APIs to get hardware information. If these APIs are modified or subverted, users will not receive correct information, such as the hardware data their application depends upon [57].

D. FIRMWARE

In distinguishing firmware from the operating system, the firmware can be the simplified startup software, bootloader, or bootstrap program that loads the operating system, and is directly installed on the hardware. As an example, BIOS is a firmware that is used daily, which checks the hardware at startup and loads the operating system. Thus, the firmware is the lowest level software that can directly take full control of the hardware. This attack surface has two kinds of vulnerabilities, the first is the same as one in the operating system layer, called the update mechanism, and the second is the device firmware attack surface.

1) UPDATE MECHANISM

This mechanism is similar to Section 2.2.2 of the operating system layer. The difference here is that, if the firmware is compromised, the results may be more serious than in the operating system layer, as an adversary has the additional capacity to directly change the hardware values and destroy the system physically.

2) DEVICE FIRMWARE

This vulnerability is based on the directly on the firmware itself. It includes only a single vulnerability, called firmware and storage extraction. Through it, an adversary can use some methods to extract useful information, including the source code, the binary file of a running service, pre-set passwords, and SSH keys, among others [69]. Typically, this means using JTAG or SWD debugging interfaces [70]. More specifically, JTAG is a standard of on-chip instrumentation in Electronics Design Automation (EDA), an industry standard for printed circuit board testing. JTAG leaves a convenient low-level backdoor for programmers to carry out testing, giving them the highest privilege and full access to the entire printed circuit board. Similarly, while the UART interface provides a higher-level software/command shell, logger output, and others distinct from JTAG, it still has a backdoor for programmers to have the highest privilege. Generally speaking, firmware and some potentially sensitive data will be stored on a portable chip, and could thus be extracted via JTAG or UART interface [71], easily granting an adversary access to the sensitive data.

E. HARDWARE

In the hardware layer, we consider the partial or full control of system hardware and potential subversion or damage. In some cases, an adversary can reach the hardware directly, such that the protection policy may not be very effective. From this perspective, we divide the attack surface into two parts: the hardware (sensors, actuators), and the device physical interface.

1) HARDWARE (SENSORS)

On this attack surface, the adversary can use various means to compromise sensors and actuators, instantiating false data to confuse the control system administrator and the decision making process. The system may then carry out incorrect decisions and damage the hardware or components of the system. An example is the Stuxnet worm, which compromises the sensors of the nuclear power generation facility and compromises the control system to destroy the nuclear power plant [72].

2) DEVICE PHYSICAL INTERFACE

This attack surface is based on the access interface between hardware and firmware. This attack surface has the following three vulnerabilities: (i) *Removal of Storage Media.* This vulnerability is based upon connected portable storage media that could be physically removed, leading to disconnection or disfunction of services, applications, or the device itself, as well as the potential for compromised portable devices to infect the devices and systems. An example is the first version of Stuxnet, which used USB devices to compromise nuclear power plants. Adversaries could also use vulnerabilities in the hardware or firmware to steal important credentials from physically extracted removable storage devices [57], [73]. (ii) *Manipulation of Device Code Execution Flow.* Manipulating the code execution flow of a device is a vulnerability that can make use of JTAG and the GNU Project debugger (GDB). The GDB enables to observe the execution of another

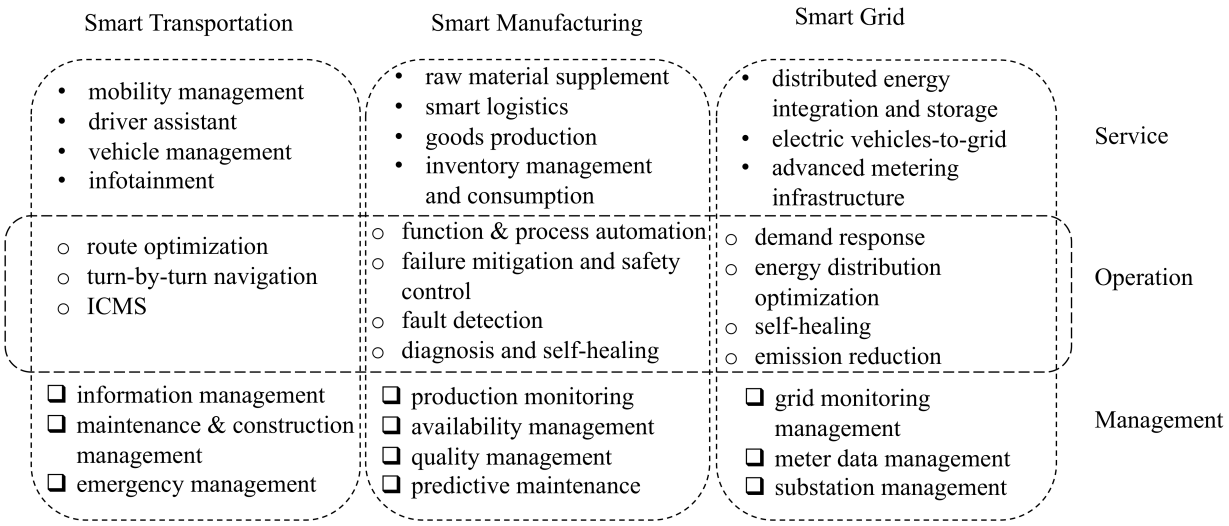

FIGURE 5. Three-layer architecture of smart transportation, Smart manufacturing, and smart grid.

program, or what a program was doing at the moment it crashed. Here, adversaries could modify the execution of firmware so that almost all software-based security controls can be bypassed [57], [73]. (iii) *Obtaining Console Access.* Obtaining console access is similar to the firmware and storage extraction vulnerability in Section 2.4.2. Here, an adversary could use some method (like UART or JTAG) to gain full access to a serial interface. Usually, security measures (e.g., custom bootloaders) are capable of preventing adversaries from going to single user mode, but these have occasionally been bypassed and are not completely secure [57], [73].

III. KEY IOT APPLICATIONS

In this section, we investigate key IoT applications, including smart transportation, smart manufacturing and smart grid, from a three-layer architecture perspective. This three-layer architecture consists of service, operation, and management layers, which represent the key components of CPS. In considering the applications and their layers, we provide individualized examples of the service, operation, and management layers in each of the applications (smart transportation, smart manufacturing, and smart grid individually).

A. SMART TRANSPORTATION

1) SERVICE LAYER

Smart transportation provisions many add-on services, including mobility management, driver assistance, vehicle management, and infotainment, among others, to enhance the driving experiences of users under the restrictions of driving safety [74]–[76]. Mobility management is intended to significantly reduce the time of different driving tasks, including finding the shortest route to a destination, assisting with parking, and so on. The driver assistant is designed to assist drivers in safely operating their vehicles, through methods such as lane change assistance and collision prevention, to name a few. Vehicle management aims to assist drivers in vehicle maintenance through mechanisms such as vehicle condition monitoring, and detecting and preventing faults, among others. For instance, Apple Carplay, as a representative infotainment system, enables full integration of information technology and mobile applications in vehicles [77]. Combined with a distraction-free interface, such integration can enable location services, navigation, infotainment, and so on to enhance the driving experience. Specifically, many infotainment services include music to relax or stimulate drivers to avoid and relieve driving fatigue. Note that driving fatigue is the cause of more than 20 % of traffic accidents [78].

2) OPERATION LAYER

In addition to the add-on services mentioned above, another key objective of smart transportation is to enable safe and efficient transportation system operations, including route optimization, turn-by-turn navigation, and information-centric multimedia streaming (ICMS), among others. Route optimization utilizes information technologies to assist drivers in computing optimal routes based on current real-time traffic conditions [4], [79], [80]. Route optimization can be configured to achieve a variety of objectives, including minimizing the average time per trip, maximizing fuel efficiency, and others. Turn-by-turn navigation assists drivers in efficiently operating their vehicles to reach their destinations. Likewise, by enabling ICMS, drivers can make timely decisions based on video streams collected from upcoming traffic locations [81].

3) MANAGEMENT LAYER

Many management systems in exist and play critical roles in smart transportation, such as information management, maintenance and construction management, and emergency management [82], [83]. Information management is concerned with the timely delivery of critical information, such as schedule, traffic, weather, and so on. Maintenance and construction

management aims to efficiently maintain transportation systems, seeking to sustain good operating conditions and minimize system downtime. Emergency management ensures the safety of drivers and pedestrians during emergency scenarios, enabled by a variety of safety functions, such as driver assisting systems (DAS), collision avoidance systems, emergency condition notifications, and vehicle health monitoring, diagnosis and maintenance, to name a few. For example, DAS can assist drivers in operating vehicles safely during emergency scenarios, such as during poor driving conditions (rain, fog, and darkness, among others). The DAS provides several features enabled by smart transportation, including real-time imaging of roads, real-time geospatial database for vehicle navigation, on-vehicle sensors to detect surroundings, and more [84]. Emergency condition notification enables a number of vehicles to participate in the broadcasting emergency messages, such that all drivers will be notified appropriately.

B. SMART MANUFACTURING

1) SERVICE LAYER

Smart manufacturing enables the interconnectivity of industrial things, including sensors, actuators, logistics, machines, etc., on a closed-loop supply chain to support many industrial services [6], [85], [86]. Key industrial services consist of raw material supply, smart logistics, goods production, inventory management, and consumption [18]. Raw material supply includes the storing, moving, and consumption of raw materials efficiently during production (e.g., producing the maximum volume of goods at minimum cost). Inventory management seeks the efficient management of production speed with regard to customer demand. Smart logistics introduces the cost-effective scheduling of massively dispersed goods delivery.

2) OPERATION LAYER

Operation of smart manufacturing (i.e., smart factories and plants) through the interconnectivity of sensors, actuators, and controllers, includes function and process automation, failure mitigation and safety control, and fault detection, diagnosis, and self-healing [87], [88]. Note that control systems that could be operated by supervisory control and data acquisition (SCADA), distributed control system (DCS), and so on, play critical roles to operate industrial systems. Function and process automation leverages seamless data collection and command dissemination to conduct continuous production processes without human intervention. Failure mitigation and safety control could prevent unsafe operation conditions, reduce health risks, and protect workers. Control systems could detect and diagnose faults automatically and induce self-healing mechanisms to recover from system faults.

3) MANAGEMENT LAYER

The management of production devices, including robotics, sensors, controllers, etc. can be improved via automation and visualization of production environments, which includes production monitoring, availability management, quality management, and predictive maintenance [89]–[91]. Production monitoring is real-time manufacturing monitoring and data collection to ensure normal operations and production efficiency of manufacturing machines and personnel. Availability management indicates the analysis and management of the availability of facilities, machinery, personnel, etc. in plants and factories to maximize their productivity and efficiency. Quality management examines the quality of the production processes and output, and identifies defective products. Finally, predictive maintenance can effectively improve productivity by reducing equipment downtime through predictive maintenance scheduling.

C. SMART GRID

1) SERVICE LAYER

The smart grid leverages and interconnects power grids, transmission lines, substations, and consumers via cutting-edge technologies, and enables a variety of services to improve reliability and efficiency, through technologies such as distributed energy integration and storage, electric vehicle-to-grid infrastructures, advanced metering infrastructure (AMI), and so on [101]–[103]. Distributed energy integration and storage combines distributed renewable-energy generation facilities (i.e., solar plants, wind turbines, thermal power facilities, etc.) with distributed energy storage facilities [9], [10], [10], [104], [105]. Such integration enables a two-way electricity power transmission (between consumers and grids) that is aware of energy demand and supply. Electric vehicle-to-grid infrastructure integrates plug-in electric vehicles with the smart grid, increasing the use of renewable-energy and reducing dependence on fossil-fuel energy resources. In addition, AMI leverages smart meters to measure, collect, and analyze energy supply and usage in real time to benefit both consumers and grids through mechanisms such as dynamic energy pricing [106].

2) OPERATION LAYER

Smart grid system operations consist of demand response, energy distribution optimization, self-healing, emission reduction, and so on to achieve efficient energy generation, transmission, and utilization [105], [107]–[109]. Demand response operation can balance power supply and demand. For example, users can transmit power (generated or stored) back into the smart grid system during peak electricity demand periods. Power distribution systems in the smart grid leverage automation technologies to transmit electricity at low cost and with high flexibility specifically for distributed energy sources. Moreover, as a key operation, self-healing enables automatic diagnosis of system failures in the smart grid and restores the system to normal operations. Moreover, enabled by the smart grid, the efficient utilization of electricity can significantly reduce energy waste and carbon emissions.

TABLE 1. Examples of attacks on smart transportation.

Attacks Targets	Definition	Example	Impacts
Denial of control action (Operation)	Disrupting the transmission of control information for vehicle operation	Jamming the signal transmission of the automotive control system between vehicles in a platoon [92]. Impeding the transmission of sensed data in a closed-loop control system [93].	Vehicles with automotive control system will not able to response to control commands.
Denial of services from core components (Operation)	Blocking or delaying information transmission from core components (e.g., RSU) to vehicles	Adversaries periodically transmit messages to collide with the RSU's periodic message broadcasting [94].	The RSUs fail to transmit time-critical information to the vehicles.
Tampering with vehicle and core component authentication (Management)	Fabricating and modification of messages (e.g., sensed data, warning messages) by illegitimate nodes	Attack on the authentication system for vehicle communication resulting in adversary masquerading as a legitimate vehicle [95]. Launch of Sybil attack to abuse and disrupt the authentication system [96].	Tampering, blocking, or delaying legitimate or emergency message transmission. Compromising the authentication system.
Spoofing vehicle status and infrastructure information (Service & Operation)	Transmitting false control signals and status information to vehicles or RSUs	In the in-vehicle controller area network (CAN), the adversary uses malicious application (e.g., self-diagnostic) to get access to control data and launch attacks [97]. The adversary spoofs sensed messages collected from the in-vehicle sensors (e.g., tire pressure sensors) in in-vehicle CAN [98].	Making in-vehicle sensors malfunction. Stealing sensitive vehicle data.
Masquerading to access (read) security-sensitive and resource data (Service & Operation)	Unauthorized access to private information of the user (driving history, destination address, planed route, etc.)	Adversaries can track vehicles based on their identification information during safety services [99].	Obtaining the location and identification information of vehicles for illegitimate purposes.
Congesting resources (Management)	Congesting networking resources and exhausting computing resources	Adversaries broadcast forged messages during the authentication process to consume computation resources of the receiver [100].	Authentication becomes unavailable, which delays or blocks legitimate tasks.

3) MANAGEMENT LAYER

Management in the smart grid includes grid monitoring management, meter data management, and substation management, among others [108], [110]. Grid monitoring improves visualization for system operators and enables the self-detection of grid instabilities. Meter data management incorporates critical information delivery, storage, and processing, including the status information for transmission and distribution systems, generation system, and more. Substation management can rapidly configure substations in the smart grid to improve the system flexibility. For example, traditionally, a main trunk carries the majority of electricity from a substation to customers, delivered through laterals. In the smart grid, however, distributed energy resources can be connected to multiple substations to enable an interconnected feeder system.

IV. CYBER-ATTACKS ON IOT APPLICATIONS

In this section, we investigate cyber-attacks on smart transportation, smart manufacturing and smart grid, and consider their impacts. In particular, for each of the three key IoT applications (i.e., smart transportation, smart manufacturing, and smart grid), we first list the cyber-attacks, outlining the attack targets, definition, examples, and impacts. We then consider in more detail the impacts of both single small-scale and complex large-scale attacks upon the service, operation, and management layers.

A. ATTACKS ON SMART TRANSPORTATION

Table 1 provides a list of attacks on smart transportation, including their definitions, impacts, and examples. In the following, we illustrate the impacts of attacks from the perspectives of a single attack and a large-scale attack on the three layers of our outlined architecture.

1) ATTACKS ON SERVICE

Koscher *et al.* [118] investigated attacks on automobiles from disabling brakes to disrupting entertainment services. In particular, they noted the lack of security protections (e.g., cryptographic mechanisms) during communication as one of the primary vulnerability risks of IoT [119]. In considering individual attacks, adversaries could attack vehicle management services (e.g., tire monitoring) by spoofing the sensed data with false data to disrupt driving [98], [120], [121]. Moreover, in a large-scale cyber-attack, a massive number of vehicles will be negatively affected. For example, adversaries could interfere with the vehicle management service (e.g., remote operation) of many vehicles.

2) ATTACKS ON OPERATION

Attacks on operations can directly result in inefficient vehicle operation and failure. For example, failure on route management leads to higher trip costs and can further result in congestion. In this case, adversaries can delay the delivery of traffic condition messages to disrupt efficient route management systems on vehicles. Considering a single small-scale attack, an adversary could launch a jamming attack to disrupt the delivery of congestion warning messages [83], [94], [122], [123]. Thus, the route optimization fails to compute an efficient route to avoid congested areas. Attacks on a large scale could lead to the inefficient operation of many vehicles and maximize the occurrence of traffic jams in times of peak travel (rush-hour traffic). For example, adversaries can launch the least-effort attacks to maximize the average

TABLE 2. Examples of attacks on smart manufacturing.

Attacks Targets	Definition	Example	Impacts
Denial of control action (Operation)	Delaying or blocking the transfer of control messages between system operator and control system	Adversaries launch DoS attack on remote state estimation [112]. Adversaries launch DoS attack on sensing loop of smart grid [113].	Degrading control performance (e.g., state estimation accuracy). Causing fluctuation in the industrial systems (e.g., power system).
Manipulate control logic (Operation)	Modifying the control software that automatically operates the control system	Adversaries can launch command injection attacks to overwrite the control logic (e.g., ladder logic in Programmable logic controller (PLC)) [114].	Overwriting programs to make PLC malfunction.
Reprogram controllers (Service & Operation)	Changing the programs of controllers that control manufacturing processes	Adversaries can change parts of the PLC program code [115].	Modifying controllers to operate irregularly or improperly.
Modify safety system (Management)	Modifying safety system to disrupt emergency management of control systems	Due to a cyber incident, the safety systems behave errantly (has been deployed to cause nuclear plant shutdown) [116].	Damaging safety protection mechanisms, which otherwise prevent control systems from achieving unsafe states (May induce unsafe states).
Spoof system status information (Operation)	Sending false system status information to system operator to induce inaccurate operation decisions	Adversaries can launch man-in-the-middle attack, sending false messages to system operators to disrupt normal operations [117].	Injecting false responses or false commands in control systems.
Malicious software (Operation)	Introducing malicious software to control systems	Adversaries introduce Stuxnet or other malware/virus/worm to compromise PLC [118].	Malicious software gains unauthorized control of the control system. Malicious software steals important and confidential data. Malicious software propagates to other devices.

delay in specific target areas with a minimum number of vehicles (i.e., delay message delivery) [124].

3) ATTACKS ON MANAGEMENT

Adversaries can launch attacks to disrupt the safety functions of smart transportation to compromise the safety of drivers and pedestrians. For instance, one real-world example is the spoofing of tire-pressure data from tire pressure sensors [97], [98], enabled by the lack of cryptographic mechanisms in communication protocols in-vehicle controller area networks (CANs). To disrupt emergency management, such as DAS, adversaries could inject false data in place of measurement data from in-vehicle sensors, such as the safe distance monitoring of adjacent vehicles, resulting in drivers making incorrect or unsafe decisions based on the false data [125]–[129]. To launch a large-scale attack, aggressive adversaries could inject false safe distance monitoring data to a number of vehicles simultaneously to cause the maximum number of accidents, which would be especially damaging during emergency scenarios. For example, under poor driving conditions, a large-scale accident could affect rescue vehicles and potentially evolve into be a public safety event.

B. ATTACKS ON SMART MANUFACTURING

In Table 2, we present examples of attacks on smart manufacturing systems, including their definitions and impacts. We next elaborate attacks and their impacts from the perspectives of both a single attack and a large-scale attack, each against the three-layer architecture.

1) ATTACKS ON SERVICE

Due to the incredible business value and investment represented in any factory or industrial system, industrial things, including equipment, machinery, and processes, are attractive targets for cyber-attacks. Adversaries can launch single attacks to disrupt industrial activities in a closed-loop supply chain, or can implement large-scale attacks to cause disturbances across many critical services. For example, adversaries can attack inventory management stations and report false inventory information (e.g., low inventory) via spoofing [116], [139], [140]. The result will be inventory management falsely placing orders based on autonomous inventory management schemes. Depending on the industry and the companys capital investments, this could severely affect the profitability and value of the target company or owning corporation. In addition, adversaries can launch large-scale attacks on many inventory management stations of a global firm to manipulate the inventory management more broadly. For example, adversaries could control compromised stations to report false inventory information to the central station with a variety of schemes, such as low inventory for low-demand areas and high inventory for high-demand areas. Thus, products will be oversupplied to low-demand areas and undersupplied to low-demand area inappropriately. This result will be greater imbalance in the supply and demand management, requiring significant wasted work to return or reallocate the products, as well as incurring many other negative impacts and overall economic loss [141].

2) ATTACKS ON OPERATION

Aggressive adversaries are likely to attack the system operations (i.e., control systems) of critical manufacturing infrastructures to steal valuable manufacturing data or cause severe damage, if they have not already. For example, an adversary could capture an industrial process controller in a chemical plant to steal critical operation and parameter settings.

TABLE 3. Examples of attacks on smart grid.

Attacks Targets	Definition	Example	Impacts
Masquerading to access (read) smart meter data and private information (Service)	Gaining unauthorized access to private information (power usage history, power usage analysis, etc.)	Adversaries can collect account or billing information through analysis of high-frequency meter data [131]. Adversaries can infer the habits of consumers via energy consumption information [132].	Unauthorized access leads to leakage of private consumer information. Consumers could face economic losses or subversion of personal safety.
Denial of service in energy distribution and transmission operations (Operation)	Interfering with or disrupting the transmission and distribution system	Adversaries launch DoS attacks on substation network in the power grid operated by the distributed network protocol (DNP3) [133].	DoS attacks degrade the performance of distribution and transmission, and disable the substation network.
Manipulating control logics (Service & Operation)	Adversaries modify the control software that autonomously controls smart appliances	Adversaries control smart appliances through large-scale IoT attacks via botnets [134]. Adversaries launch DoS attacks to alter energy load (i.e., increase power usage) [135].	This attack can damage grid devices, cause local outages, large-scale blackouts, and increase operational costs.
Spoof system status (Service & Operation)	Transmitting false control signals and data to smart grid devices	Adversaries launch spoof attacks on the energy distribution system (i.e., power demand information) [136]. Adversaries inject false meter data to manipulate market pricing [137].	Manipulation and disruption of energy distribution systems and energy markets.
Disrupt authentication in smart grid (Management)	Fabricating and modifying information (e.g., power usage, price information) by illegitimate nodes	Tampering with the price signal in demand response systems [138]. Adversaries send old (previously sent) messages to launch a replay attack [139].	Disrupted or manipulated pricing in energy markets to mislead demand and response.
Congesting network resources (Management)	Cause networking resources to be unavailable to deliver messages in a timely manner	Adversaries launch jamming attacks to delay or completely block the delivery of time-critical messages [140].	Jamming attacks degrade and disable energy supply and distribution management systems.

In addition, adversaries can launch large-scale attacks on multiple control systems to cause severe damage. For example, the Stuxnet worm was utilized to access critical program logic controllers on Irans nuclear plant to caused substantial damage [117], [142]–[145]. As another example, adversaries could substitute false data for critical variables, such as pressure and temperature in massively deployed actuators, monitors, ovens, crucibles, etc. in chemical plants, resulting in hazardous public safety events, such as chemical release. Clearly, cyber-attacks on large-scale industrial plants, such as chemical plants, oil plants, and nuclear plants, can cause significant destruction, and even loss of life.

3) ATTACKS ON MANAGEMENT

In a massively connected environment enabled by industrial IoT, adversaries and bad actors will be motivated by self-interest or competition to steal the valuable production information (e.g., type and volume of material productions) and even disrupt the production process to their benefit. For example, adversaries could launch individual attacks to capture sensors that identify defects in production on assembly lines via node capture attack. In this way, the adversaries could conduct illegitimate activities, adversely affect the defect rate, or simply collect valuable business data (e.g., estimated defective rate) for illegal trade or benefit. In addition, adversaries could launch large-scale attacks to circumvent or disable unified quality management services of factories that belong to a global firm or competitor [143], [146]–[150]. The target would then be unable to accurately measure defects, possibly leading to overestimation of product quality and the production of a massive number of defective products, causing immense economic loss.

C. ATTACKS ON SMART GRID

In Table 3, we list a variety of attack examples against the smart grid, providing their definitions and impacts. In the following, we illustrate the impacts of attacks in more detail from the perspectives of single small-scale and large-scale attacks for each of the three architecture layers.

1) ATTACKS ON SERVICE

Komninos [8] investigated a number of attacks on smart grid from direct load shifting to meter data manipulation. Specifically, as single, small-scale attacks, adversaries can control certain IoT devices, such as home appliances, in the smart grid. Using their control, an adversary can induce an abnormal working state in the device, increasing the power usage of the household. In certain cases, aggressive adversaries can cause damage to the devices and their surroundings, and even threaten the personal safety of users [134], [151]–[153]. In terms of large-scale cyber-attacks, adversaries can compromise many high-wattage IoT devices to manipulate the power demand in a larger smart grid. For example, Soltan [133] demonstrated a large-scale attack model on real-world grids, using a botnet to turn on and off a large number of IoT devices synchronously, resulting in massive power fluctuations with the potential to cause a large-scale blackout.

2) ATTACKS ON OPERATION

Cyber-attacks can directly disrupt smart grid operations through disruption of transmission and distribution systems,

demand response systems, and others [154]–[157]. For example, in a single attack, an adversary can launch a spoofing attack on the distribution system to disable the power supply [135]. In particular, by spoofing the Global Positioning System (GPS) components installed in measurement devices in the smart grid, adversaries can provide false power demand information to the grid. Thus, normal operations in the smart grid will be disrupted. In addition, in a large-scale attack, adversaries can launch a DoS attack on the power substation network via the distributed network protocol (DNP3) [132]. For example, adversaries could use traffic flood attacks to delay the transmission of messages, using legitimate but useless user datagram protocol (UDP) traffic to occupy the communication channel. As a result, substation networks would be overloaded with heavy traffic, negatively impacting power grid transmission and distribution.

3) ATTACKS ON MANAGEMENT

Adversaries can launch attacks on the management layer of the smart grid to degrade system performance and cause the financial losses to both supply and demand interests [158]–[161]. As a single attack, an adversary could send old energy usage messages in a replay attack [8]. The supply side would receive inaccurate demand information and manage or adjust their supply incorrectly. At the same time, demand side users would fail to accurately capture their consumed electricity. In terms of large-scale attacks, adversaries could jam time-critical messages (e.g., price, power usage) to disrupt or incapacitate the entire power market. For example, adversaries could jam the power price and price change signals [137], [162]. Consumers who are affected by the attack will then take actions in response to the incorrect change or lack of change in the price of electricity. Adversaries could also predict the direction of changes and manipulate the price in the electricity market to disrupt smart grid management or achieve financial benefits. The abrupt change of power consumption due to costumer behavior will also negatively impact smart grid stability.

V. A CASE STUDY FOR INVESTIGATING CYBER-ATTACKS ON THE SMART TRANSPORTATION SYSTEM

We now present a case study investigating the least-effort attack on the smart transportation system as an example to study the impacts of cyber-attacks on IoT systems. In particular, we study the attack impacts for different scales of attack, using the percentage of compromised smart transportation devices to quantize the attack scale. Note that the least-effort attack is intended to induce the most damage to the target (smart transportation system) while compromising the least number of devices (on-board and road-side units), thereby using an optimum or minimum volume of resources. In this scenario, we consider that adversaries can disrupt the vehicular network of the smart transportation system using a denial-of-service attack by, while controlling the least number of compromised vehicles necessary. In addition, adversaries can disrupt vehicle traffic and cause congestion via manipulating a minimum number of Road-Side Units (RSUs), such as traffic lights. In the following, we present our simulation setup and the evaluation results.

A. EXPERIMENTAL SETUP

We assume that adversaries can successfully attack smart transportation devices, such as On-Board Units (OBUs) and smart traffic lights. Note that the OBU is a central unit of a smart vehicle that interfaces with driver to collect information and handle message transmission. In this simulation, we assume that adversaries can directly manipulate message transmission and the frequencies of traffic lights. Nonetheless, the adversary cannot directly control the behaviors of drivers.

In this setup, we first consolidated a comprehensive testbed, composed of OMNET++, Veins, and SUMO [163]. The Simulation of Urban Mobility (SUMO) is an open-source, continuous traffic simulator that can simulate vehicle traffic in a variety of parameters, with variable parameters such as the number of vehicles, road, vehicle speed, and so on. OMNET++ is a highly scalable network simulation framework that can integrate with many different modules. Veins is an open source framework that can integrate OMNET++ and SUMO to capture the interactions of vehicular networks and vehicle traffic. The communication protocol implemented for this simulation is 802.11p [163].

In the implementation of our simulation, we use a map of Towson, Maryland, USA to model real-world road topologies, as shown in Fig. 6. Additionally, in modeling traffic, we consider that vehicles could either enter or exit the main road from any possible side roads. Furthermore, we randomly generate the vehicles and their routes. The full list of our simulation parameters is presented in Table 4, and includes simulation area, simulation time, number of trials, vehicles, and traffic lights.

To carry out the simulation study, we first use SUMO to generate the vehicle motion information. We then transfer the motion information to OMNET++ in real-time via transmission control protocol (TCP) port. Next, in OMNET++, we mount network modules to each vehicle. For convenience, we call these communication-ready vehicles nodes, which broadcast packets to all other nodes that within their range. With this setup, we ran the simulation 200 times to get the baseline of normal traffic conditions with zero compromised nodes, designated as normal operation.

B. ATTACK SCENARIOS

We now introduce the three attack scenarios investigated in this case study.

Attack on the vehicular network in the smart transportation system via compromised OBUs. Adversaries compromise nodes to disrupt the vehicular network by broadcasting redundant messages (e.g., replay attack). Note that normal nodes can broadcast the same message up to three times. Nonetheless, the compromised nodes will repeatedly broadcast the same message. Under this mechanism, we

FIGURE 6. Road topology of the towson area generated by SUMO simulator.

TABLE 4. Simulation Parameters.

Attacks Targets	Definition
Simulation Area	5000 x 3100 m^2
Simulation Time (Each Trial)	5000 s
Number of Trials	120
Number of Vehicles	200
Network Protocol	802.11p
Number of Traffic Lights	300
Attack Strategies	Low frequency, Random frequency, High frequency
Network Interface	OMNET++
Vehicular Network Simulation Framework	Veins
Traffic Simulator	SUMO
Map	Towson University

consider the following three attack strategies that can be leveraged by adversaries: (i) uniform distribution attack in which adversaries randomly compromise nodes with a uniform distribution, (ii) density-based attack in which adversaries always compromise nodes with the highest node density (i.e., the largest number of nodes in their communication range), and (iii) advanced density-based attack in which adversaries divide the road topology into many small areas and compromise nodes by highest node density in those areas.

Attack on the vehicle traffic in the smart transportation system via compromised RSUs (i.e., traffic lights). Adversaries compromise traffic lights to disrupt vehicle traffic (i.e., increase traffic congestion). Manipulating traffic lights to frequently change between stop and go, the overall travel delay will increase. Furthermore, using specific control logic, vehicles could be locked in certain areas. We assume that all vehicles will comply with the instructions of traffic lights. Under this mechanism, we design three attack strategies by implementing the following three distinct traffic light frequencies: (i) low frequency (i.e., the adversaries manipulate all traffic lights at a low frequency), (ii) random (i.e., the induced light transition frequencies are random), and (iii) high frequency (i.e., the induced frequency is rapid).

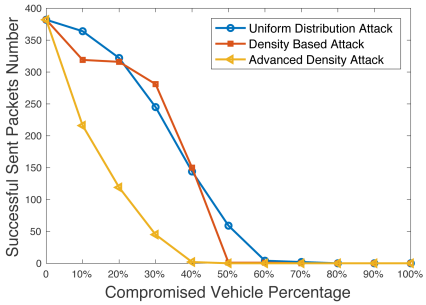

FIGURE 7. Results of attacks on vehicular network via compromised OBUs.

Combined attack on the vehicular network and vehicle traffic in the smart transportation system via compromised OBUs and RSUs. Adversaries disrupt smart transportation system via manipulating both traffic lights and vehicle nodes to cause maximum damage with minimum cost.

C. EVALUATION RESULTS

Attack on the vehicular network in the smart transportation system via compromised OBUs. In assessing the impacts of this attack, we compare the network performance of the three attack strategies (i.e., uniform distribution attack, density-based attack, and advanced density-based attack). The network performance is measured by number of packets successfully received. As shown in Fig. 7, to completely paralyze the network, an adversary does not necessarily need to compromise all nodes. Because the normal nodes will rebroadcast messages sent by compromised nodes, the attack can successfully occupy the channel resources to paralyze the network. We can also observe that, to completely paralyze the network, adversaries using the uniform distribution attack need to compromise the largest number of nodes, followed by the density-based attack, and advanced density attack. When network paralysis is not maximized, we can see that the uniform distribution and density-based attacks behave very similarly, while the advanced density-based attack is clearly much more effective.

Regarding the uniform distribution attack, adversaries need to compromise more nodes to ensure that the attack can affect every node in the network. Because the vehicle trajectory is random and mobility is high, compromised nodes will not stay within communication range of other nodes for long. Thus, the impact of nodes compromised under uniform distribution is limited. In the density-based attack, adversaries can generally attack more nodes with fewer compromised nodes, because, on average, there are more nodes near compromised nodes. Nonetheless, one issue for the density-based attack is that compromised nodes are typically close together, which yields distinct stages in the effectiveness of the attack. This also explains why the results of the uniform distribution attack are better than when 20 %-40 % of vehicles are compromised. Finally, owing to the advanced density-attack dividing the global attack area into smaller sub-areas,

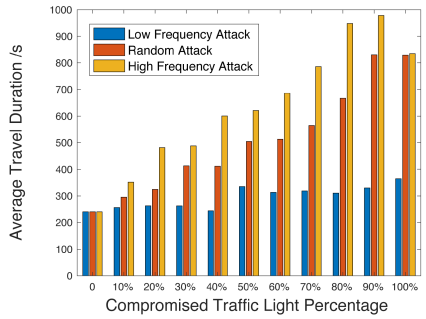

FIGURE 8. Average travel duration during attacks on vehicle traffic via compromised RSUs (i.e., traffic lights).

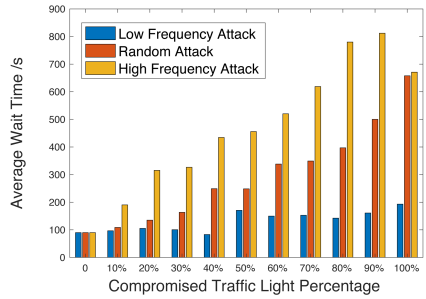

FIGURE 9. Average wait time during attacks on vehicle traffic via compromised RSUs (i.e., traffic lights).

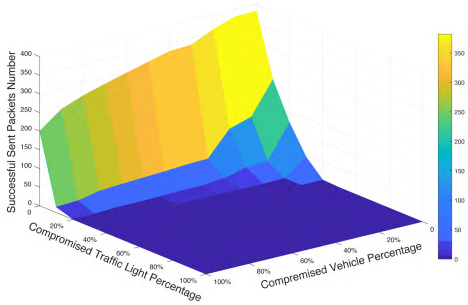

FIGURE 10. Successful sent packets number during attacks on vehicular networks via compromised OBUs and RSUs.

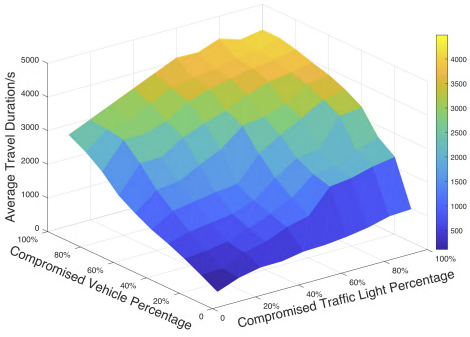

FIGURE 11. Average travel duration during attacks on vehicular traffic via compromised OBUs and RSUs.

this attack avoids the problem of compromised nodes being clustered in the same area. Thus, the advanced density-based attack achieves better performance with fewer compromised nodes to disrupt whole network.

Attack on the vehicle traffic in the smart transportation system via compromised RSUs (i.e., traffic lights). In this evaluation, we assess the impacts of attacks on traffic light frequencies (i.e., low, random, and high frequency) by comparing average travel durations and average wait times. Average travel duration is calculated as the average time from start to finish for all the vehicles to complete their routes. Additionally, the average wait time is calculated as the average time spent for all vehicles at a speed of less than 0.1 m/s. Combining both, we can sufficiently evaluate traffic congestion in various areas.

In Fig. 8, we observe that manipulating traffic lights at a high frequency results in the highest average travel durations, in comparison with random and low frequency manipulation. When the traffic lights are induced to change with high frequency, the vehicles have a lower likelihood of driving through the intersection without slowing down, passively reducing the speed of all vehicles. In addition, as shown in Fig. 9, vehicles will remain effectively stopped in the same place for longer. Indeed, the average wait time is increased significantly, especially under the high-frequency scheme, indicating that many vehicles were locked in a particular area for a long duration.

Attack on the vehicular network and vehicle traffic in the smart transportation system via compromised OBUs and RSUs. Recall that, in a smart transportation system, objects such as OBUs and RSUs are interconnected to maximize information sharing. The combined attack strategy (i.e., manipulating both OBUs and RSUs) can make the most of this trait to optimize and maximize the leverage of an attack. Note that compromised traffic lights can restrict vehicles to a particular area for a longer duration. Also, compromised vehicles can effectively disable the vehicle network. Thus, adversaries can compromise vehicles to broadcast false traffic messages in addition to manipulating traffic lights to maximize traffic congestion.

In this evaluation, we assess the performance of the combined attack strategy to paralyze the network and maximize traffic congestion. In particular, taking the most effective of both attack mechanisms, we combine the manipulation of traffic lights at high frequency with the advanced density-based attack on vehicles. As shown in Fig. 10, with only a small number of compromised traffic lights, the effectiveness of the compromised vehicle attack (i.e., disruption of network performance) is greatly increased. For example, when 10 % of traffic lights were compromised, the number of compromised nodes needed to disrupt entire network decreased by 10 % in comparison with no compromised traffic lights. Similarly, when 30 % of traffic lights were compromised, the number of compromised nodes required to disrupt entire network decreased by 20 % from the baseline.

Simultaneously, the addition of compromised vehicles can improve the efficiency of attacks against vehicular traffic (i.e.,

average travel duration) in comparison to only manipulating traffic lights. As shown in Fig. 11, compromising 30 % of vehicles nearly doubles the average travel duration compared with the baseline. In summary, the hybrid attack strategy cause maximum damage to the target (i.e., operations in smart transportation) compared to the single domain attack strategies.

VI. RESEARCH OPPORTUNITIES

In this section, we discuss some research opportunities, outlining a series of research problems that need to be resolved as critical foundations to address the security issues raised by widespread IoT adoption. These research opportunities can be considered from a traditional three-phased security assessment framework that includes: (i) investigating risks of cyber-attacks, (ii) designing defensive schemes, and (iii) leveraging integrated evaluation platforms to protect IoT-based systems against cyber-attacks.

A. RISKS OF CYBER-ATTACKS

The investigation of vulnerabilities (e.g., software vulnerabilities, communication vulnerabilities, side-channel vulnerabilities) can help system designers to understand the security risks inside a particular system, and can be used explore adversarial models likely to be used in launching cyber-attacks. To investigate system vulnerabilities, the development of taxonomies to systematically explore potential vulnerabilities in smart grid, smart transportation, and smart manufacturing systems, and others, have been studied [9], [164], [165]. Despite the similarity of architectures in these key IoT-based systems, the service, operation and management of these systems are uniquely different. Thus, the investigation of vulnerabilities in IoT-based systems must be conducted on a case-by-case basis.

With an understanding of potential vulnerabilities, the potential impacts of those vulnerabilities on specific key functions in the studied systems must also be investigated. For example, the impacts of vulnerabilities in power flow control, demand response, and energy pricing in the smart grid, traffic management, location-based service, and driving safety in the smart transportation system, as well as process control, real-time monitoring, and product inspection in the smart manufacturing system should be clearly assessed. Taking the smart grid as an example, an adversary could fully control smart plugs [166] to disrupt optimal power flow control by turning smart plugs on and off rapidly and repeatedly to generate misleading demand reports, leading to inefficient load management, as well as to cause power fluctuations the may result in grid blackouts.

Further, we should consider that an adversary will consider manipulating a variety of assorted parameters (e.g., the duration for launching attacks, spatial distribution of IoT devices, and the number of devices to be compromised) to achieve their attack goals in time, space, and strength. Thus, it becomes necessary to model and analyze the impacts of attacks that consider various combinations of factors (attack parameters, strategies, etc.) in time, space, and strength. For instance, an investigation should be conducted to find optimal strategies for selecting a set of smart plugs to compromise and the magnitudes of their controlled outputs needed to maximize the attack damage. With these strategies, the risks inherent to the system can be established, and intelligent defensive schemes can be devised.

B. DEFENSIVE SCHEMES

The design of defensive schemes to protect against cyber-attacks and secure IoT-based systems is another critical issue. Generally speaking, defensive schemes can be allocated into four processes: (i) designing resilient IoT-based systems, (ii) investigating optimal IoT-based system configurations, (iii) detecting cyber-attacks effectively, and (iv) responding to cyber-attacks in a timely manner.

First, from the perspective of system design, a resilient IoT-based system requires tamper-resistant hardware and resilient firmware and software. It is incumbent on the manufacturers of IoT devices to apply adequate security techniques to all components of their products, including software, hardware, and communication components, such that, once implemented in any system, the user has confidence that the manufactured devices are secure. In addition, it is incumbent on any system designer to apply security best-practices and understand the limitations of the devices implemented in their system. To better achieve these needs, it is necessary to develop taxonomies for techniques to secure IoT devices (e.g., securing software, improving the security of communication components, and others). Moreover, while the investigation of protection mechanisms to implement in IoT-based systems, making them difficult to compromise, have been investigated [5], [167], [168], more work is needed.

As an example of enhancing the resilience of a component, we can enhance the resilience of the Kalman filter techniques [169], enabling the component to adapt to noise dynamically and better handle certain attacks. Particularly, when the predicted measurement and received measurement deviate significantly, it could increase the absolute residual vector subsequently increases the measurement noise so that Kalman gain can be reduced. This will reduce the weight of received measurements in the estimation and preserve the estimation performance. Conversely, if the deviation between the predicted measurement and received measurement is small, the reduction in absolute residual vector shall raise only marginal change in the measurement noise, yielding only a small impact on the estimation results.

Additionally, the investigation of modeling results and their adaptation into the design of resilient systems from physical and network structures and components must be considered. On important strategy is to design protection mechanisms that increase attack costs. Using the power grid as an example, to make the power grid more resilient to attacks [5], improving the resiliency of particular critical sensors to against attacks has been proposed, which increases attack costs based on the power grid structure model. That is,

because power grids usually cover large geographical areas, it is more practical for system operators to choose some ''important sensors and actuators'' from the entire set of meters to protect, which leverages the integration of cryptography, threat monitoring and control, and other mechanisms. For example, using the IEEE 14-bus system to conduct experiments, Yang *et al.* [5] demonstrated that, when particular buses were secured, the number of state variables that adversaries must manipulate to affect an attack was significantly increased, in contrast to when buses were protected at random. In this case, applying more costly and complex security mechanisms to a few components may be more cost effective than securing all components with less costly mechanisms.

Moreover, to ensure the safe operation of IoT systems, optimal system configurations for IoT-based systems must be investigated. Specifically, IoT device placement, monitoring, control, software update and maintenance scheduling, and so on must be considered in tandem. The diverse services enabled by disparate IoT-based systems may be highly dependent on optimal system configuration, including the optimal deployment of key components. For example, the optimal deployment strategy for phasor measurement units (PMUs) in the smart grid has been considered to secure other nearby smart grid IoT devices, and is able to defend against the false data injection attacks [37]. In this case, the optimal strategy for false data injection attacks was formulated using a least-effort attack model and the design of PMU deployment strategies demonstrated the ability to defend against these data integrity attacks. Additionally, the deployment of PMUs enabled system observability with low overhead [37]. In a similar manner, it is critical to explore these and other methods for securing IoT-based systems more broadly and in scenarios generic to all CPS domains.

In the design of effective anomaly detection schemes, it is necessary to leverage both spatial and temporal correlations [5], [162], [170]–[172], along with the recent advance of big data analysis and machine learning [173], [174]. In terms of spatially-based detection, the application of machine learning and statistical schemes are possible based on the understanding that, to cause damage to IoT-based systems, the behavior of compromised sensors and malicious actuators must deviate more from the mean behavior than devices under regular use with random noise. In terms of temporally-based detection, it is well understood that adversaries may launch slow and stealthily attacks (e.g., stealthily and marginally manipulating sensors and actuators over time to cause damage over a long period of time). As a difficult strategy to identify and defend against, it is necessary to consider schemes such as nonparametric cumulative sum schemes to handle such stealthy attacks. These method accumulate small deviations in the observed sensors and actuators until the value approaches a given threshold. Advanced machine learning techniques (deep learning, etc.) should also be considered and applied in detecting cyber-attacks in IoT-based systems [173], [174], together with the assistant of distributed computing infrastructure such as edge/fog computing [3]. The effectiveness of detection algorithms can be characterized by detection rate, false positive rate, detection time, and other metrics related to attack damage and impact on critical infrastructure systems.

It is also imperative to study efficient techniques to detect compromised IoT devices. For example, to attack smart meters, an adversary could launch an attack via sending malicious code propagating traffic over the network so that malicious code can be injected into other devices. Thus, it is critical to consider perspectives such as software behavior and network traffic so that detection accuracy can be improved. Once an attack is detected, schemes must be in place to identify compromised devices and isolate them. For example, one such scheme has been proposed to adopt an efficient watermarking-based forensic trace-back scheme [165]. In this scheme, a covert signal (binary bits of 1 and 0) is used to embedded into the meter data stream. When the meter data stream is changed by any compromised device within the transmission path, the receiver can conduct a similarity-based correlation test based on the embedded covert signal to decide whether the data stream has been manipulated by adversary. Via repeating such a procedure over the data transmission path, the origin of the manipulated data can be traced.

Finally, after the cyber-attacks have been successfully detected, response plans must be in place to minimize damage to IoT-based systems and recover them from attacks. To minimize attack impacts, the isolation of the disrupting devices must be carried out while maintaining key services and operational functions. There are a variety of methods available to recover service, operation, and management to normal conditions, and these should be investigated and applied such that the response is implemented in a timely manner.

C. INTEGRATED EVALUATION PLATFORMS

To understand the risks of cyber-attacks on IoT-based systems and validate the effectiveness of defensive schemes, it is necessary to design an integrated evaluation testbed. As an IoT-based system comprises components from both the physical domain and the cyber domain, it is critical to develop system-level modeling and simulation tools to study the interactions between physical components (power grid, transportation system, and manufacturing system) and cyber components (communication networks and computing infrastructure). An integrated simulation platform can capture the interactions and reciprocal effects between communication networks and physical systems, which can be used to evaluate attack impacts on the performance and security of communication networks and computing infrastructures in IoT-based systems.

In designing and implementing a an IoT co-simulation platform, taking the smart grid as an example, the Fenix framework for Network Co-Simulation (FNCS) [11] developed by PNNL, which integrates both GridLAB-D and NS-3, is a strong candidate. FNCS is an open source co-simulation tool for studying interactions between cyber components and power grid applications. It can be used to study how the

performance of the network will impact the effectiveness of the smart grid as a whole. More specifically, using FNCS, we can describe the interactions between the power grid, communication networks, and computational algorithms, and characterize the uncertainties raised by cyber-attacks by compromising actuators (e.g., smart plugs) and sensors.

Another example is the integrated testbed utilized in the case study outlined above, which includes OMNET++, SUMO, and Veins for simulating vehicular networks in the smart transportation system [45]. Here, OMNET++ is a network simulator that can model the communication network for mobile nodes, such as vehicles. The simulation of urban mobility (SUMO) can generate various parameters to describe vehicle networks, including traffic flows, traffic density, road topologies, and vehicle speed, among others. Finally, Veins is a framework to capture the interactions between vehicular communication network and road traffic, tying the other two components together. Using this integrated testbed, we can capture the interactions between vehicular networks and the transportation system, and characterize the impacts of cyber-attacks by compromising vehicles and RSUs (e.g., traffic lights), as demonstrated.

Additionally, the wireless cyber-physical simulator (WCPS), which integrates Simulink and TOSSIM, can capture interactions between physical systems and wireless sensor and actuator networks [46]. The Simulink component of WCPS can model, simulate, and analyze multi-domain dynamic systems, such as process control systems, structural control systems, and others [46], [175], [176]. Meanwhile, TOSSIM simulates TinyOS wireless sensor networks, capturing data delivery between sensors and base stations. In WCPS, the sensed data will be fed to controllers based on the captured data delivery performance (i.e., loss and delay) to model the actuating domain. With WCPS, we can describe the interactions between manufacturing systems and wireless sensor and actuator networks, and characterize the impacts of cyber-attacks by compromising actuators (e.g., controllers) and sensors.

VII. FINAL REMARKS

In this paper, we have provided a detailed consideration of the security of IoT-based critical infrastructures. Specifically, we have considered a broad range of vulnerabilities that adversaries could exploit to intrude in critical systems. We have assessed three key IoT smart-systems applications, namely Smart Transportation, Smart Manufacturing, and the Smart Grid from the perspective of a three-tiered architecture of service layer, operation layer, and management layer. We have provided a variety of attack types for each application and layer, as well as examples for every case. Additionally, we have carried out a case study, using the Smart Transportation system as an example, that considered the impacts of attacks of varying strengths and types, and demonstrated the efficacy of least effort attacks in crippling complex IoT systems. Finally, we have outlined some research opportunities for security risk assessment, developing countermeasures, and designing integrated evaluation platforms to evaluate the impacts of attacks and the effectiveness of countermeasures.

ACKNOWLEDGMENT

Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agency.

REFERENCES

[1] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[3] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[4] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A novel dynamic en-route decision real-time route guidance scheme in intelligent transportation systems," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, Jun./Jul. 2015, pp. 61–72.

[5] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[6] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[8] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[9] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Washington, DC, USA, 2012, pp. 183–192. doi: 10.1109/ICCPS.2012.26.

[10] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema, "Toward integrating distributed energy resources and storage devices in smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 192–204, Feb. 2017.

[11] P. Moulema, W. Yu, D. Griffith, and N. Golmie, "On effectiveness of smart grid applications using co-simulation," in *Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2015, pp. 1–8.

[12] *Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions)*, Statista, Hamburg, Germany, Nov. 2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[13] J. Fruhlinger, "The mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet," IDG Commun., Framingham, MA, USA, Tech. Rep., Mar. 2018. [Online]. Available: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[14] *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication*, Food Drug Admin., Silver Spring, MD, USA, Jan. 2017. [Online]. Available: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

[15] A. Gregg, "Defense industry grapples with cybersecurity flaws in new weapons systems," Washington Post, Washington, DC, USA, Tech. Rep., Oct. 2018. [Online]. Available: https://www.washingtonpost.com/business/economy/defense-industry-grapples-with-cybersecurity-flaws-in-new-weapons-systems/2018/10/14/b1de3bae-ce36-11e8-a360-85875bac0b1f_story.html?noredirect=on&utm_term=.aca68ca687f1

[16] *Gao-19-128 Weapon Systems Cybersecurity: Dod Just Beginning to Grapple With Scale Of Vulnerabilities*, Government Accountab. Office, Washington, DC, USA, Oct. 2018. [Online]. Available: https://www.gao.gov/assets/700/694913.pdf

[17] S. A. Morse, "Investigation: Wannacry cyber attack and the NHS," National Audit Office, London, U.K., Tech. Rep. 5-10, May 2017. [Online]. Available: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
[18] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
[19] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, and J. Terpenny, "Cybersecurity for digital manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 3–12, Jul. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0278612518300396
[20] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "Towards a systematic survey of industrial IoT security requirements: Research method and quantitative analysis," in *Proc. ACM Workshop Fog Comput. IoT*, 2019, pp. 56–63.
[21] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," *IEEE Trans. Ind. Informat.*, to be published.
[22] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, to be published.
[23] S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten, and T. Newe, "Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions," *Future Gener. Comput. Syst.*, vol. 93, pp. 596–608, Apr. 2019.
[24] R. Antrobus, B. Green, S. A. F. Frey, and A. Rashid, "The forgotten I in IIoT: A vulnerability scanner for industrial Internet of Things," in *Proc. Living Internet Things*, 2019.
[25] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404812000429
[26] D. Goodin, "Feds: Hospital hacker's 'massive,' DDoS averted: Arrest foils 'devil's day' scheme," Register, Tech. Rep., Jul. 2009. [Online]. Available: https://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested/
[27] J. Wan, J. Liu, Z. Shao, A. V. Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in Internet of vehicles," *Sensors*, vol. 16, no. 1, p. 88, 2016. [Online]. Available: http://www.mdpi.com/1424-8220/16/1/88
[28] J. Lin, W. Yu, N. Zhang, X. Yang, and L. Ge, "Data integrity attacks against dynamic route guidance in transportation-based cyber-physical systems: Modeling, analysis, and defense," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8738–8753, Sep. 2018.
[29] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870517300562
[30] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Sii-mobility: An IoT/IoE architecture to enhance smart city mobility and transportation services," *Sensors*, vol. 19, no. 1, p. 1, 2019.
[31] S. Mahmood, R. Hasan, A. Ullah, and K. U. Sarker, "SMART security alert system for monitoring and controlling container transportation," in *Proc. 4th MEC Int. Conf. Big Data Smart City (ICBDSC)*, Jan. 2019, pp. 1–5.
[32] A. Lei, Y. Cao, S. Bao, P. Asuquom, H. Cruickshank, and Z. Sun, "Blockchain-based dynamic key management for IoT-transportation security protection," *IEEE Internet Things J.*, p. 117, 2019.
[33] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[34] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 21–32. doi: 10.1145/1653662.1653666.
[35] J. Lin, W. Yu, and X. Yang, "Towards multistep electricity prices in smart grid electricity markets," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 286–302, Jan. 2016.
[36] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, "Toward data integrity attacks against optimal power flow in smart grid," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1726–1738, Oct. 2017.
[37] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1735–1750, Jul. 2017.
[38] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Secur. Commun. Netw.*, vol. 9, no. 9, pp. 833–849, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.835
[39] S. Bhattarai, L. Ge, and W. Yu, "A novel architecture against false data injection attacks in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 907–911.
[40] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.
[41] M. S. Obaidat, S. P. Rana, T. Maitra, D. Giri, and S. Dutta, "Biometric security and Internet of Things (IoT)," in *Biometric-Based Physical and Cybersecurity Systems*. Springer, 2019, pp. 477–509.
[42] A. Tiwari, R. P. Tripathi, and D. Bhatia, "Advancements in data security and privacy techniques used in IoT-based hospital applications," in *Medical Data Security for Bioengineers*. Hershey, PA, USA: IGI Global, 2019, pp. 185–207.
[43] F. Kammüller, O. O. Ogunyanwo, and C. W. Probst, "Designing data protection for gdpr compliance into iot healthcare systems," 2019, *arXiv:1901.02426*. [Online]. Available: https://arxiv.org/abs/1901.02426
[44] R. Francis, "Ransomware makes healthcare wannacry," IDG Commun., Framingham, MA, USA, FTech. Rep., May 2017. [Online]. Available: https://www.csoonline.com/article/3196827/data-breach/ransomware-makes-healthcare-wannacry.html
[45] H. Noori, "Realistic urban traffic simulation as vehicular ad-hoc network (VANET) via veins framework," in *Proc. IEEE 12th Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2012, pp. 1–7.
[46] Y. Ma, D. Gunatilaka, B. Li, H. Gonzalez, and C. Lu, "Holistic cyber-physical management for dependable wireless control systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 3, no. 1, p. 3, 2018.
[47] Open Web Application Security Project. (Dec. 2018). *IoT Vulnerabilities Project*. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities
[48] Securebox. *Man in the Middle Attack (MITM)*. Accessed: Oct. 11, 2018. [Online]. Available: https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/
[49] R. E. Navas, H. Le Bouder, N. Cuppens, F. Cuppens, and G. Z. Papadopoulos, "Demo: Do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*, Saint-Malo, France, Sep. 2018, pp. 1–6. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01893999
[50] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-capable IoT malwares: Comparative analysis and Mirai investigation," *Secur. Commun. Netw.*, vol. 2018, Feb. 2018, Art. no. 7178164. doi: 10.1155/2018/7178164.
[51] Cloudflare. *Memcached DDoS Attack*. Accessed: Oct. 21, 2018. [Online]. Available: https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/
[52] M. Šimon, L. Huraj, and T. Horák, *DDoS Reflection Attack Based on IoT: A Case Study*. Cham, Switzerland: Springer, 2019, pp. 44–52.
[53] P. Čisar and S. M. Cisar, "General vulnerability aspects of Internet of Things," in *Proc. IEEE 16th Int. Symp. Comput. Intell. Inform. (CINTI)*, Nov. 2015, pp. 117–121.
[54] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *Proc. 3rd Int. Conf. Electron. Design (ICED)*, Aug. 2016, pp. 321–326.
[55] J. Hall and A. Bichsel, "Account lockout threshold," Microsoft, Tech. Rep., Nov. 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold
[56] B. Schneier, "Two-factor authentication: Too little, too late," *Commun. ACM*, vol. 48, no. 4, p. 136, Apr. 2005. doi: 10.1145/1053291.1053327.
[57] M. Stanislav and T. Beardsley, "HACKING IoT: A case study on baby monitor exposures and vulnerabilities," Rapid7, Boston, MA, USA, Tech. Rep. 6-7, Sep. 2015. [Online]. Available: https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[58] M. Elkhodr, S. Shahrestani, and H. Cheung, "A contextual-adaptive location disclosure agent for general devices in the Internet of Things," in *Proc. IEEE 38th Annu. Conf. Local Comput. Netw.-Workshops*, Oct. 2013, pp. 848–855.

[59] J. S. Kumar and D. R. Patel, "A survey on Internet of Things: Security and privacy issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, Mar. 2014.

[60] A. Tierney. (May 2018). Z-Shave. Exploiting Z-Wave Downgrade Attacks, Pen Test Partners LLP. [Online]. Available: https://www.pentestpartners.com/security-blog/zshave-exploiting-z-wave-downgrade-attacks/

[61] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 1313–1328.

[62] L. Tung. (Jul. 2018). *Bluetooth Security: Flaw Could Allow Nearby Attacker to Grab Your Private Data*. [Online]. Available: https://www.zdnet.com/article/bluetooth-security-flaw-could-allow-nearby-attacker-to-grab-your-private-data/

[63] J. Hayes. (Aug. 2015). *Zigbee's Wireless Security Flaws Threatens IoT Devices*. [Online]. Available: https://eandt.theiet.org/content/articles/2015/08/zigbees-wireless-security-flaws-threatens-iot-devices/

[64] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2014, pp. 1244–1248.

[65] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol, Version 1.2*, document RFC 5246, IETF, Aug. 2008. [Online]. Available: https://www.ietf.org/rfc/rfc5246.txt

[66] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[67] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[68] M. B. Barcena and C. Wueest, "Security response: Insecurity in the Internet of Things," Symantec, Mountain View, CA, USA, Tech. Rep. 10-14, Mar. 2015. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

[69] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (VITAE)*, Feb. 2011, pp. 1–5.

[70] *JTAG*. Accessed: Oct. 13, 2018. [Online]. Available: https://en.wikipedia.org/wiki/JTAG#Serial_Wire_Debug

[71] *Universal Asynchronous Receiver-Transmitter*. Accessed: Oct. 12, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter

[72] *Stuxnet*. Accessed: Oct. 19, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Stuxnet

[73] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[74] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 241–246.

[75] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social Internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, Mar. 2015.

[76] H. Xu, J. Lin, and W. Yu, *Secure and Trustworthy Transportation Cyber-Physical Systems*. 2017, pp. 23–49.

[77] R. Glon and M. Branman. (Jul. 2018). *What is Apple CarPlay?* [Online]. Available: https://www.digitaltrends.com/cars/what-is-apple-carplay/

[78] Transport Accident Commission. *Avoiding Driver Fatigue*. Accessed: Oct. 30, 2018. [Online]. Available: https://www.tac.vic.gov.au/road-safety/safe-driving/tips-and-tools/fighting-fatigue

[79] W. Li, G. Wu, D. Yao, Y. Zhang, and M. J. Barth, "Dynamic en-route eco-navigation: Strategy design, implementation and evaluation," in *Proc. IEEE 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 1888–1893.

[80] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET—A survey," *IEEE Trans. Intell. Transp. Syst.*, to be published.

[81] W. Quan, C. Xu, J. Guan, H. Zhang, and L. A. Grieco, "Social cooperation for information-centric multimedia streaming in highway VANETs," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2014, pp. 1–6.

[82] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: Sensing-aided transportation information collection and diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3813–3825, May 2018.

[83] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing," *IEEE Access*, vol. 7, pp. 1570–1585, 2019.

[84] M. Donath and C. Shankwitz, "Driver assistive system—Assistance in low visibility conditions," Univ. Minnesota, Minneapolis, MN, USA, Tech. Rep., 2018. [Online]. Available: http://license.umn.edu/technologies/z00053_driver-assistive-system-assistance-in-low-visibility-conditions

[85] A. Kusiak, "Smart manufacturing," *Int. J. Prod. Res.*, vol. 56, nos. 1–2, pp. 508–517, 2018.

[86] J. Oh and B. Jeong, "Tactical supply planning in smart manufacturing supply chain," *Robot. Comput.-Integr. Manuf.*, vol. 55, pp. 217–233, Feb. 2019.

[87] A. Caggiano, "Cloud-based manufacturing process monitoring for smart diagnosis services," *Int. J. Comput. Integr. Manuf.*, vol. 31, no. 7, pp. 612–623, 2018.

[88] S. Rahimifard, J. Stone, P. Lumsakul, and H. Trollman, "Net positive manufacturing: A restoring, self-healing and regenerative approach to future industrial development," *Procedia Manuf.*, vol. 21, pp. 2–9, Jan. 2018.

[89] F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-driven smart manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 157–169, Jul. 2018.

[90] C. W. Kang, M. B. Ramzan, B. Sarkar, and M. Imran, "Effect of inspection performance in smart manufacturing system based on human quality control system," *Int. J. Adv. Manuf. Technol.*, vol. 94, nos. 9–12, pp. 4351–4364, 2018.

[91] Q. P. He and J. Wang, "Statistical process monitoring as a big data analytics tool for smart manufacturing," *J. Process Control*, vol. 67, pp. 35–43, Jul. 2018.

[92] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[93] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, Mar. 2017.

[94] S. Biswas, J. Mišić, and V. Mišić, "DDoS attack on WAVE-enabled VANET through synchronization," in *Proc. Global Commun. Conf.*, Dec. 2012, pp. 1079–1084.

[95] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Proc. Comput., Commun. Appl. Conf. (ComComAp)*, Jan. 2012, pp. 345–350.

[96] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[97] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[98] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. 19th USENIX Conf. Secur. (USENIX)*. Berkeley, CA, USA: USENIX Association, 2010, p. 21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929848

[99] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[100] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," in *Proc. IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE)*, vol. 3, May 2012, pp. 261–265.

[101] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[102] C.-S. Wang and P. Li, "Development and challenges of distributed generation, the micro-grid and smart distribution system," *Automat. Electr. Power Syst.*, vol. 34, pp. 10–14 and 23, 2010.

[103] H. Rahimi-Eichi, U. Ojha, F. Baronti, and M.-Y. Chow, "Battery management system: An overview of its application in the smart grid and electric vehicles," *IEEE Ind. Electron. Mag.*, vol. 7, no. 2, pp. 4–16, Jun. 2013.

[104] M. Wolsink, "The research agenda on social acceptance of distributed generation in smart grids: Renewable as common pool resources," *Renew. Sustain. Energy Rev.*, vol. 16, no. 1, pp. 822–835, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032111004564

[105] D. An, Q. Yang, W. Yu, X. Yang, X. Fu, and W. Zhao, "SODA: Strategy-proof online double auction scheme for multimicrogrids bidding," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 7, pp. 1177–1190, Jul. 2018.

[106] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On data integrity attacks against real-time pricing in energy-based cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, pp. 170–187, Jan. 2017.

[107] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 82–88, Jun. 2010.

[108] R. E. Brown, "Impact of smart grid on distribution system design," in *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Elect. Energy 21st Century*, Jul. 2008, pp. 1–4.

[109] X. Gao and X. Ai, "The application of self-healing technology in smart grid," in *Proc. Asia–Pacific Power Energy Eng. Conf.*, Mar. 2011, pp. 1–4.

[110] P. Zhang, F. Li, and N. Bhatt, "Next-generation monitoring, analysis, and control for the future smart control center," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 186–192, Sep. 2010.

[111] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[112] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (DoS) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Feb. 2013, pp. 1–6.

[113] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Res. Summit*, Oct. 2010, pp. 1–9.

[114] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proc. AsiaCCS*, 2011, pp. 355–366.

[115] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," Washington Post, Washington, DC, USA, Tech. Rep., Jun. 2008. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

[116] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IEEE 37th Annu. Conf. Ind. Electron. Soc. (IECON)*, Nov. 2011, pp. 4490–4494.

[117] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier: Version 1.4," Symantec Secur. Response, Melbourne, VIC, Australia, Tech. Rep., Feb. 2011. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[118] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[119] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things security 'hands-on,'" *IEEE Security Privacy*, vol. 14, no. 1, pp. 37–46, Jan./Feb. 2016.

[120] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Vehicle security: Risk assessment in transportation," 2018, *arXiv:1804.07381*. [Online]. Available: https://arxiv.org/abs/1804.07381

[121] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, Nov. 2018.

[122] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[123] T. Limbasiya and D. Das, "Secure smart vehicle cloud computing system for smart cities," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Springer, 2018, pp. 395–415.

[124] Ş. Okul, M. A. Aydin, and F. Keleş, "Security problems and attacks on smart cars," in *Proc. Int. Telecommun. Conf.* Springer, 2019, pp. 203–213.

[125] M. U. Rehman, S. Ahmed, S. U. Khan, S. Begum, and S. H. Ahmed, "Performance and execution evaluation of vanets routing protocols in different scenarios," *EAI Endorsed Trans. Energy Web*, vol. 5, no. 17, p. e14, 2018.

[126] A. N. Upadhyaya and J. Shah, "Attacks on VANET security," *Int. J. Comput. Eng. Inf. Tech.*, vol. 9, no. 1, pp. 8–19, 2018.

[127] X. Cheng and B. Huang, "A center-based secure and stable clustering algorithm for VANETs on highways," *Wireless Commun. Mobile Comput.*, vol. 2019, Jan. 2019, Art. no. 8415234.

[128] E. S. Stolyarova, D. M. Shiryaev, A. G. Vladyko, and M. V. Buinevich, "VANET/ITS cybersecurity threats: Analysis, categorization and forecasting," in *Proc. IEEE Conf. Russian Young Res. Elect. Electron. Eng. (EIConRus)*, Jan./Feb. 2018, pp. 136–141.

[129] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, "A survey on sybil attack detection in vehicular ad hoc networks (VANET)," *J. Comput.*, vol. 29, no. 2, pp. 1–6, 2018.

[130] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.

[131] F. G. Mármol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 166–172, May 2012.

[132] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proc. MILITARY Commun. Conf. (MILCOM)*, Oct./Nov. 2010, pp. 1830–1835.

[133] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Conf. Secur. Symp. (SEC)*, 2018, pp. 15–32. [Online]. Available: http://dl.acm.org/citation.cfm?id=3277203.3277206

[134] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[135] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[136] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: Attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.

[137] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 1168–1172.

[138] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1871–1879.

[139] Y. Cui, F. Bai, Y. Liu, P. Fuhr, and M. Morales-Rodriguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Trans. Smart Grid*, to be published.

[140] S. R. Chhetri, S. Faezi, N. Rashid, and M. A. Al Faruque, "Manufacturing supply chain and product lifecycle security in the era of industry 4.0," *J. Hardw. Syst. Secur.*, vol. 2, no. 1, pp. 51–68, 2018.

[141] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018.

[142] M. Holloway, "Stuxnet worm attack on iranian nuclear facilities," Stanford Univ., Stanford, CA, USA, Tech. Rep. 54,56, Jul. 2015. [Online]. Available: http://large.stanford.edu/courses/2015/ph241/holloway1/

[143] L. Sha, F. Xiao, W. Chen, and J. Sun, "IIoT-SIDefender: Detecting and defense against the sensitive information leakage in industry IoT," *World Wide Web*, vol. 21, no. 1, pp. 59–88, 2018.

[144] H. Wang, Z. Zhang, and T. Taleb, "Special issue on security and privacy of iot," *World Wide Web*, vol. 21, no. 1, pp. 1–6, 2018.

[145] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.

[146] S. Adepu and A. Mathur, "Distributed attack detection in a water treatment plant: Method and case study," *IEEE Trans. Dependable Secure Comput.*, to be published.

[147] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput.*, vol. 71, pp. 66–77, Oct. 2018.

[148] S. Madhawa, P. Balakrishnan, and U. Arumugam, "Roll forward validation based decision tree classification for detecting data integrity attacks in industrial Internet of Things," *J. Intell. Fuzzy Syst.*, vol. 36, no. 3, pp. 2355–2366, 2019.

[149] M. Zolanvari, M. A. Teixeira, and R. Jain, "Effect of imbalanced datasets on security of industrial iot using machine learning," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Nov. 2018, pp. 112–117.

[150] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.

[151] R. Chen, X. Li, H. Zhong, and M. Fei, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing*, vol. 344, pp. 73–81, Jun. 2019.

[152] C. Cameron, C. Patsios, P. Taylor, and Z. Pourmirza, "Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3010–3019, May 2018.

[153] S. Khan, R. Khan, and A. H. Al-Bayatti, "Secure communication architecture for dynamic energy management in smart grid," *IEEE Power Energy Technol. Syst. J.*, vol. 6, no. 1, pp. 47–58, Mar. 2019.

[154] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[155] A. Gusrialdi and Z. Qu, "Toward resilient operation of smart grid," in *Smart Grid Control*. Springer, 2019, pp. 275–288.

[156] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[157] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 163–178, Jan. 2016.

[158] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Jan. 2010, pp. 1–7.

[159] P. Gope and B. Sikdar, "Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1554–1566, Jun. 2019.

[160] S. M. Kim, T. Lee, S. Kim, L. W. Park, and S. Park, "Security issues on smart grid and blockchain-based secure smart energy management system," in *Proc. MATEC Web Conf.*, vol. 260, 2019, Art. no. 01001.

[161] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," 2018, *arXiv:1806.00121*. [Online]. Available: https://arxiv.org/abs/1806.00121

[162] X. Yang, X. Zhang, J. Lin, W. Yu, X. Fu, and W. Zhao, "Data integrity attacks against the distributed real-time pricing in the smart grid," in *Proc. IEEE 35th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2016, pp. 1–8.

[163] H. Noori, "Realistic urban traffic simulation as vehicular Ad-hoc network (VANET) via Veins framework," in *Proc. 12th Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2012, pp. 1–7.

[164] W. Yu, "False data injection attacks in smart grid: Challenges and solutions," in *Proc. NIST Cyber Secur. Cyber-Phys. Syst. Workshop (CPS)*, 2012, pp. 1–51.

[165] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie, "An integrated detection system against false data injection attacks in the smart grid," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 91–109, 2015.

[166] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of Internet of Things: A case study of the smart plug system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017.

[167] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[168] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2551–2566, Mar. 2017.

[169] G. Valverde and V. Terzija, "Unscented Kalman filter for power system dynamic state estimation," *IET Generat., Transmiss. Distrib.*, vol. 5, no. 1, pp. 29–37, Jan. 2011.

[170] X. He, X. Yang, J. Lin, L. Ge, W. Yu, and Q. Yang, "Defending against energy dispatching data integrity attacks in smart grid," in *Proc. IEEE 34th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2015, pp. 1–8.

[171] J. Lin, W. Yu, and X. Yang, "On false data injection attack against multistep electricity price in electricity market in smart grid," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 760–765.

[172] X. Yang, X. Zhang, J. Lin, W. Yu, and P. Zhao, "A Gaussian-mixture model based detection scheme against data integrity attacks in the smart grid," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–9.

[173] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.

[174] W. G. Hatcher and W. Yu, "A survey of deep learning: Platforms, applications and emerging research trends," *IEEE Access*, vol. 6, pp. 24411–24432, 2018.

[175] B. Li, Z. Sun, K. Mechitov, G. Hackmann, C. Lu, S. J. Dyke, G. Agha, and B. F. Spencer, "Realistic case studies of wireless structural control," in *Proc. ACM/IEEE Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2013, pp. 179–188.

[176] Y. Ma and C. Lu, "Efficient holistic control over industrial wireless sensor-actuator networks," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Oct. 2018, pp. 89–98.

XING LIU received the B.S. degree from the Shanghai University of Engineering Science, Shanghai, China, in 2016, and the M.S. degree in electrical and computer engineering from Lawrence Technological University, in 2018. He is currently pursuing the Ph.D. degree with Towson University. His research interests include machine learning, the Internet of Things, and cybersecurity.

CHENG QIAN received the B.S. degree from Jianqiao University, Shanghai, China, in 2018. He is currently pursuing the M.S. degree with Towson University. His research interests include the Internet-of-Things, cyberspace security and privacy, and computer networks.

WILLIAM GRANT HATCHER received the B.Sc. degree in materials science and engineering from the University of Maryland and the master's degree in computer science from Towson University, in 2018, where he is currently pursuing the Ph.D. degree. His research interests include mobile computing and security, big data, and machine learning.

HANSONG XU received the B.S. degree from the City College, Xi'an Jiaotong University, Xi'an, China, in 2013, and the M.S. degree in electrical engineering from Lawrence Technological University, in 2016. He is currently pursuing the Ph.D. degree with Towson University. His research interests include computer networks, the Internet of Things, and machine learning. He received the Graduate Student Research Award and the Doctorial Research Fellowship, in 2018.

WEIXIAN LIAO received the B.S. degree in information engineering from Xidian University, Xi'an, China, in 2012, the M.S. degree in electrical and computer engineering from Mississippi State University, Starkville, MS, USA, in 2015, and the Ph.D. degree in computer engineering from Case Western Reserve University, Cleveland, OH, USA, in 2018. He is currently an Assistant Professor with the Department of Computer and Information Sciences, Towson University. His research interests include cybersecurity and optimization in big data applications, cyber physical systems, and machine learning.

WEI YU received the B.S. degree in electrical engineering from the Nanjing University of Technology, Nanjing, China, in 1992, the M.S. degree in electrical engineering from Tongji University, Shanghai, China, in 1995, and the Ph.D. degree in computer engineering from Texas A&M University, in 2008. He was with Cisco Systems, Inc., for nine years. He is currently a Full Professor with the Department of Computer and Information Sciences, Towson University, MD, USA. His research interests include cyberspace security and privacy, cyber-physical systems, the Internet of Things, and big data. He was a recipient of the 2014 NSF Faculty CAREER Award, the 2015 University System of Maryland (USM) Regents' Faculty Award for Excellence in Scholarship, Research, or Creative Activity, and the University System of Maryland (USM)'s Wilson H. Elkins Professorship Award, in 2016. His work has also received Best Paper Awards from IEEE ICC 2008, ICC 2013, IEEE IPCCC 2016, and WASA 2017.