Journal of Network and Computer Applications 132 (2019) 118–148

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey

Abhishek Gupta [a], Alagan Anpalagan [a,*], Glaucio H.S. Carvalho [c], Ahmed S. Khwaja [a], Ling Guan [a], Isaac Woungang [b]

[a] Dept. of Electrical and Computer Engineering, Ryerson University, Toronto, Canada
[b] Dept. of Computer Science, Ryerson University, Toronto, Canada
[c] Faculty of Applied Science and Technology (FAST), Sheridan College Institute of Technology and Advanced Learning, Oakville, Canada

ARTICLE INFO

Keywords:
Internet of things
Smart grid
Advanced persistent threats
Intrusion detection systems
Security
Privacy
Cyber kill-chain

ABSTRACT

This paper presents a comprehensive survey of existing as well as evolving security threats and vulnerabilities and the state-of-the-art countermeasures in Internet of Things (IoT)-enabled smart grids. The cybersecurity risks in smart grid networks and associated devices prevail in the form of malicious use leading to data espionage, physical damage to devices, intentional denial of service and exploitation for financial gain. We begin with an introduction to IoT and data transfer techniques between different devices, and their role and significance in the growth of smart grids. We then discuss privacy concerns, and various attack motives with which intruders try to break into smart grids. This is followed by a classification of threat actors in modern networks based on the sophistication of attacks they can launch. We also provide a classification of threat vectors in smart grids including attacks against integrity, attacks against availability, attacks against privacy and attacks against authentication. In addition, we investigate the nature and extent of risk posed by advanced persistent threats and the significance of deploying next generation intrusion detection systems in smart grids. The seven-step attack procedure known as cyber kill-chain is discussed and current detection, prevention, and access control measures in practice are also summarized in form of tables. These tables would help the reader correlate prevalent and futuristic attack techniques, countermeasures, and the applicability, scalability and feasibility of current security mechanisms to smart grids for achieving effective cyber hygiene. The paper then introduces novel attack surfaces that inevitably get established due to various cutting-edge communication techniques used in smart grids. One such mechanism discussed in this paper is time sensitive networking that injects the possibility of harnessing time as an attack surface. Based on the current survey, several recommendations for further research are discussed at the end of this paper.

1. Introduction

The current paradigm of ubiquitous connectivity and wireless data transfer among everyday objects continues to thrive as a technological phenomenon of modern computing. The number of connected things is on the rise and it is expected to reach 30 billion by 2020 in the form of smart grids, connected vehicles, smart cities, smart homes, smart health-care and other everyday objects which are collectively known as the Internet of Things (IoT) (Bartoli et al., 2011). The advances in wireless communication, cloud computing and virtualization, and miniaturization of cyber-physical devices have led to the adoption of Internet in some of the most critical aspects of daily life (Bartoli et al., 2011). Moreover, devices equipped with numerous sensors gather contextual information and propagate it to the neighboring nodes to facilitate a dedicated task, with reduced or minimal human intervention (Das et al., 2018). A basic IoT system embedded with device-to-device (D2D) communication is represented in Fig. 1.

The IoT applications are classified into Industrial Internet of Things (IIoT), Internet of Everything (IoE), and Social Internet of Things (SIoT) (Dacier et al., 2014). The IIoT extends the IoT technology to enterprises and industries leading to new business models based on cloud connectivity, with the bulk of data transfer being between the IoT edge components and the data stored in the cloud (Das et al., 2018). Industry 4.0, also referred to as the fourth industrial revolution, is

* Corresponding author.
E-mail address: alagan@ee.ryerson.ca (A. Anpalagan).

https://doi.org/10.1016/j.jnca.2019.01.012
Received 11 July 2018; Received in revised form 20 November 2018; Accepted 12 January 2019
Available online 5 February 2019

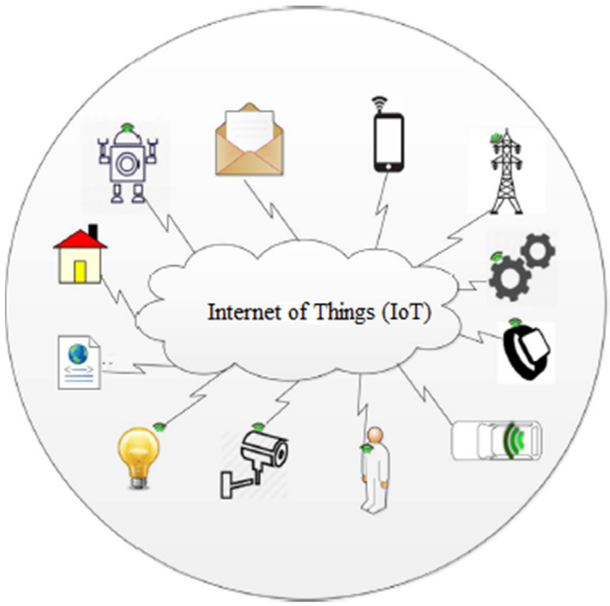


Fig. 1. An overview of connected objects in IoT architecture (Das et al., 2018).

data-communication based modern automation and manufacturing industry (Chakhchoukh and Ishii, 2015). It consists of cyber-physical systems (CPS) (Liu et al., 2015), IoT, and cognitive cloud computing (Das et al., 2018). The IoE aims to utilize improved connectivity to increase comfort in daily life through communication between ordinary devices (Chakhchoukh and Ishii, 2015). The SIoT is a version of IoT where things establish social relationships with other objects, without the need for human intervention (Chakhchoukh and Ishii, 2015). The transition of computing trends through the era of mainframe, personal computer, ubiquitous and pervasive computing towards ever connected IoT is expected to power the smart grid, which is a revolutionary technology permeating the power generation and distribution industry (Das et al., 2018).

Conventionally, power generation takes place at a small number of large power stations usually located at the outskirts or isolated regions of a city. The generated power is transmitted over high voltages and delivered at lower voltages to the end users (Bartoli et al., 2011). The distribution is one-directional from the grid to the end-user. This is known as build and connect, as once a building is built, electric network is installed with anticipated load requirements and the infrastructure is expected to last for a considerable time (Dacier et al., 2014). However, recent issues with global warming have motivated nations, businesses and researchers to discover alternate ways while gradually shifting away from the build and connect culture.

Smart grids constitute connect and manage architecture that is rapidly changing electric power landscape (Bartoli et al., 2011). In short, smart grids are an innovative interconnection infrastructure that incorporates and embeds digital intelligence in the process of generating, distributing, pricing and consuming electrical energy (Brown et al., 2012). Smart grids are largely being viewed as a possible solution to future energy problems and a crucial step towards solving global warming (Brown et al., 2012). The adoption of Internet and innovative information and communication technology (ICT) in energy sector has ushered electricity generation and distribution into a new era of change, uncertainty as well as cyberattacks (Abawajy et al., 2018). As an ICT enabled energy distribution network, smart grids are a salient foundational and characteristic feature in digital transformation of the energy sector (Dacier et al., 2014). Smart grids differ from traditional electric grids as they are equipped with the ability to monitor the electricity flow outside as well as within itself and dynamically adapt to the ambient energy-conditions (Ippolito et al., 2014). Fig. 2 illustrates perception and D2D communication in a three-tier IoT-enabled smart grid system.

This reconfiguration from conventional electric grid to modern day smart grid is based on the self-aware and context-aware information that enables smart grids to exert larger control over demand, generation and distribution (Wade et al., 2010). Smart grids provide better overall visibility into the distribution network while incorporating novel mechanisms to intelligently and proactively manage demand-generation behavior illustrated by consumers (Dacier et al., 2014). Smart grids are increasingly being perceived as the building blocks to smart cities, IoT and IIoT applications (Wang et al., 2017). To fully emerge as the power source for smart homes and smart cities, it is envisaged that the smart grids need to undergo a complete overhaul of existing association between generation, distribution, transmission and supply stakeholders, and the existing commercial, municipal, provincial, and federal regulations (Das et al., 2018). Fig. 3 delineates the bidirectional data and information flow among various components of smart grids. As with any networked device, the vulnerability to cyber threats, attackers and malicious exploitation is a critical issue that needs to be adequately addressed for avoiding catastrophic consequences in smart grids. The wide area network (WAN), neighborhood area network (NAN) and home area network (HAN) data, and the end-user IoT devices constitute the bulk of information flow in smart grids (Butun et al., 2014), (Xiao et al., 2013b), as shown in Fig. 3.

1.1. Motivation

It is estimated that by 2030, approximately 80 percent of the world's population will live in urban areas (Wade et al., 2010). The way energy is utilized in these environments is set to heavily impact the way we live, work and function as a community. Today, electricity is used when needed and unlike other energy sources, it is difficult to store electricity, except using generators (Hur, 2013). Additionally, smart grids lead to fewer brown outs, less flickering, natural power re-routing, less interference with communication systems and other electronics, enable adjustment to varying load requirements, and reduce outages (Ma et al., 2018). However, with more networked devices, ICT, and mobile workforce, smart grids are exposed to threats and must be safeguarded by introducing security during design. To analyze smart grid vulnerabilities, it is imperative to investigate some of the drivers behind the need to develop smart grids as well the conspicuous benefits for distributors, consumers and other stakeholders (Srivastava et al., 2018). One of the key concerns that arises with the digitization of devices and objects is to develop reliable mechanisms to ensure secure and trusted data transmission (Butun et al., 2014). Amidst requirements such as efficiency, self-reliance, uninterrupted ad hoc communication, robustness, scalability, adaptability and reliability, one major concern in smart grids and connected devices is secure data transmission (Ge et al., 2017). Although the communicating entities in the IoT network play a significant role in assisting human activities and industrial processes, the increased connectivity and data transfer also create avenues for misuse and exploitation leading to severe consequences (Koo et al., 2017).

Connected devices lead to increased availability of attack surfaces for breaking into a secure and critical network infrastructure (Wade et al., 2010). To mitigate the risk posed by security flaws and vulnerabilities, it is of utmost importance to detect the security issues at the earliest. Moreover, it is statistically infeasible for a smart grid and IoT network to be completely immune to cybersecurity threats as the threat landscape continues to evolve and the attackers persist to devise newer, sophisticated and organized means to break into a secure network (Kim and Tong, 2013). Smart grids cybersecurity requirements differ considerably from industrial control systems (ICS), and the supervisory control and data acquisition (SCADA) systems, due to a high number of interconnected and integrated components (Cherdantseva et al., 2016). Smart grids contribute widely to continuous operations of critical infrastructure. Increased complexity and connectivity expose them to threats and vulnerabilities risking safety and reliability (Kim and Tong, 2013). Some

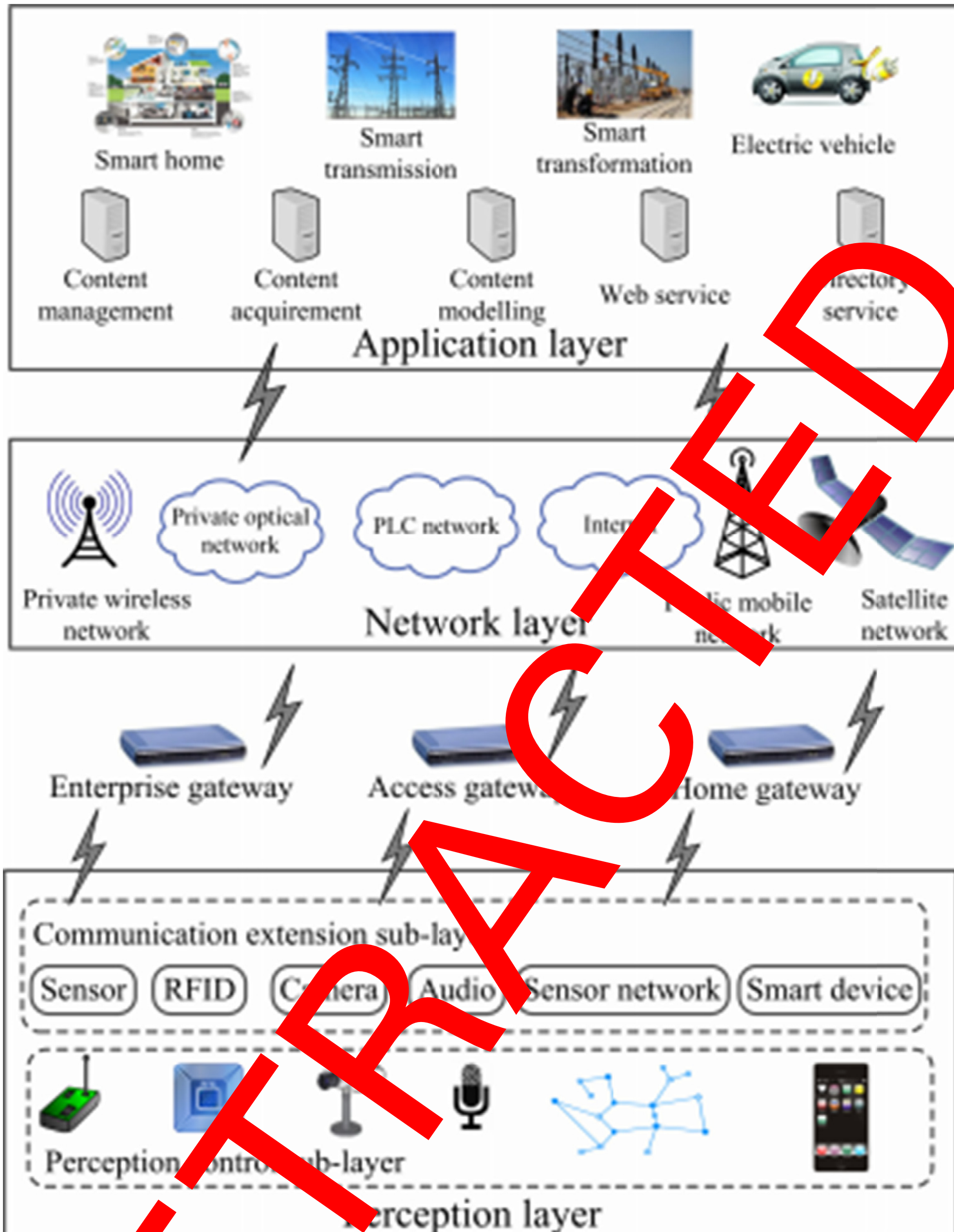


Fig. 2. Three-layered architecture of IoT-aided smart grid architecture (Fadlullah et al., 2018).

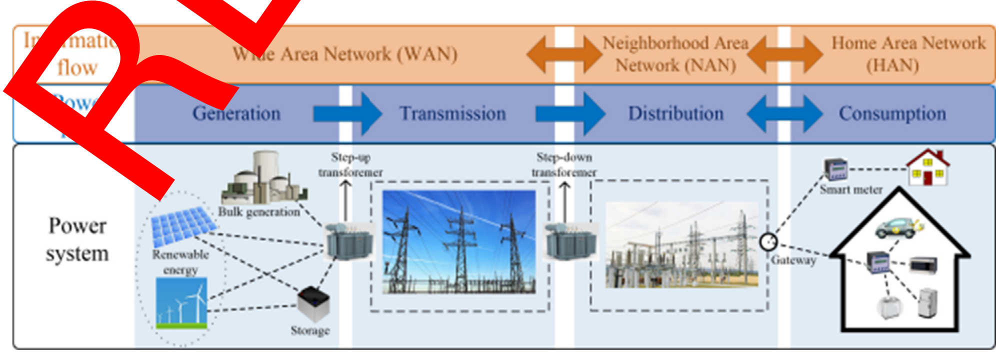


Fig. 3. Power generation, transmission, distribution, and utilization framework in IoT-enabled smart grid architecture (Xiao et al., 2013b).

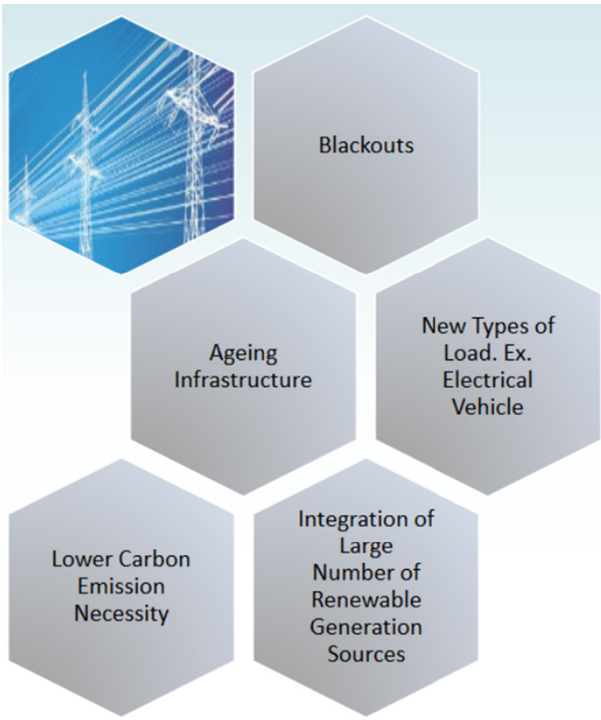


Fig. 4. The need for smart grids, potential benefits and susceptibilities (Koundinya et al., 2016).

of the factors driving the adoption of smart grids in the energy sector are depicted in Fig. 4 (Koundinya et al., 2016).

Cyberattacks and their far-reaching impacts emphasize the need to revisit security and privacy considerations in critical infrastructure (Barreto et al., 2014). The IoT networks are increasingly being used as an attack platform to launch IoT-based cyberattacks targeting devices powered by smart grids (Xiang et al., 2017). As the volume of data communication to and from smart grid ICT-network continues to grow massively, it also opens opportunities for malicious exploitation of smart grids, associated IoT devices, and sensitive information (Li et al., 2015). With connected expansion, it becomes imperative to ensure that all cybersecurity policies and mechanisms are designed, deployed, and updated consistently to guarantee safety (Srivastava et al., 2018). Smart grids equipped with comprehensive and state-of-the-art security measures ensure heightened security, resilience to attacks and vulnerabilities, accuracy of data, and increased convenience in daily lives (Wang et al., 2016a). The principal ideas motivating this survey are as follows:

- To explore the differences in cybersecurity requirements in SCADA, ICS, smart grids, and IoT-enabled smart grids (Sherdantseva et al., 2016).
- To study existing security measures, vulnerabilities, and threat addressing mechanisms in smart grids (Sun et al., 2018).
- To investigate the pattern of emerging threats and evolving security mechanisms in IoT, smart grids, and IoT-enabled smart grids (Batamuliza, 2018).
- To study applicable security measures widely adopted in SCADA and ICS that can be extended to smart grids either as they are or with some amendments (Alcaraz et al., 2011).
- To explore security vulnerabilities in smart grids that could lead to catastrophic scenarios (Wang and Lu, 2013).

1.2. Contributions of this survey article

To the best of our knowledge, this is the first time the current and prevailing security trends, and emerging cybersecurity threats in IoT-enabled smart grids are surveyed. Furthermore, the prevalent security techniques have been compared to the seven step cyber-kill chain process (Wang et al., 2016b). In this survey, we comprehensively cover the open issues, challenges and future research directions for cybersecurity trends in IoT-aided smart grid systems. The contributions of this survey are summarized as follows:

- A survey of the intersection of IoT and smart grids, i.e., IoT-enabled smart grids.
- A detailed discussion on existing security requirements for IoT systems, smart grids, and IoT-enabled smart grids.
- A detailed discussion on the existing and emerging vulnerabilities, threats, adversaries and security trends in smart grids;
- A discussion on the attack procedure, known as cyber kill-chain used to launch attacks in critical infrastructure.
- A discussion on threat actors and attack motives posing threats to smart grids.
- An overview of IoT and non-IoT communication technologies, and associated threat vectors in smart grids.
- A presentation of the open issues, challenges and future research directions in cybersecurity requirements of IoT-enabled smart grids.

Table 1 presents a list of recurring acronyms used in this paper.

1.3. Comparison with existing survey articles

In this work, unlike existing survey articles, we explore the security vulnerabilities, threats, threat actors, threat vectors, and current security trends in smart grids (Bekara, 2014). We also analyze how these prevalent security measures offer comprehensive protection against specific steps of cyber-kill chain (Wang et al., 2016b). We survey some of the security gaps and the need for futuristic or next generation tamper proof security measures (Khan and Salah, 2018). We further highlight some cybersecurity challenges that need more attention to enable development and adoption of an integration of IoT and smart grids in the future (Leszczyna, 2018b). While there exist a number of separate surveys on the IoT, smart grids, and cybersecurity trends in IoT and smart grids, to the best of our knowledge, there is no existing survey that covers emerging threats and security threats in the intersection of IoT and smart grids, and compares them to widespread practices in securing critical infrastructure such as SCADA and ICS. This survey differs from previous individual surveys on IoT and smart grids and combines IoT and smart grids, and covers emerging threats, vulnerabilities, and evolving security requirements in IoT-aided smart grids (Chin et al., 2017). A number of surveys on related topics that have contributed to this survey are shown in Table 2.

Several existing surveys have investigated security requirements, cryptography, key management, authentication, access control, and challenges to efficiently secure IoT (Alaba et al., 2017; Mendez Mena et al., 2018; Sha et al., 2018; Kouicem et al., 2018). Recently, researchers have examined the application of similar techniques to smart grid communications (Bartoli et al., 2011; Nitti et al., 2014; Militano et al., 2017). However, these studies pertain to M2M communications between different components in a sophisticated hybrid of smart networks. We explore the applicability of prevalent security principles to detect and prevent malicious attacks and intrusion attempts obfuscated in seemingly legitimate communication, targeted at exploiting a smart grid. Many studies have studied the evolution of malware, advanced persistent threat (APTs), attack mechanisms, and vulnerability of smart grids to APTs (Wang et al., 2016b; Auty, 2015; Sood and Enbody, 2013; Lemay et al., 2018; Chen et al., 2018) and a number of surveys have reviewed cybersecurity standards for smart grids and IoT. We investigate the exiting literature to study the attack patterns used by malicious threat actors. A significant component of our work is the study of a seven-step attack strategy known as cyber kill-chain and the scalability of prevalent cybersecurity techniques to safeguard against various steps of an

Table 1
List of recurring acronyms and corresponding definitions

Acronyms	Definitions
6LoWPAN	IPv6 over Low-power Wireless Personal Area Networks
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AMI	Advanced Metering Infrastructure
ANM	Active Network Management
APT	Advanced Persistent Threats
AVC	Automatic Voltage Control
CIA	Confidentiality, Integrity, and Availability
CnC	Command and Control
CPS	Cyber-Physical Systems
D2D	Device-to-Device
DARPA	Defense Advanced Research Projects Agency
DD	Dynamic Demand
DER	Distributed Energy Resource
DG	Distributed Generation
DL	Deep Learning
DLR	Dynamic Line Rating
DoS	Denial-of-Service
DR	Demand Response
FAN	Field Area Network
HAN	Home Area Network
HIDS	Host Intrusion Detection Systems
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems - Cyber Emergency Response Team
ICT	Information & Communication Technology
IDS	Intrusion Detection Systems
IED	Intelligent Electronic Device
IIoT	Industrial Internet of Things
IoE	Internet of Everything
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IPv6	Internet Protocol version 6
KDD	Knowledge Discovery in Databases
LoWPAN	Low-power Wireless Personal Area Networks
LLN	Low Power and Lossy Networks
M2M	Machine-to-Machine
MITM	Man in the Middle
ML	Machine Learning
NAN	Neighborhood Area Network
NED	Network Edge Devices
NFC	Near Field Communication
NGF	Next Generation Firewall
NIDS	Network Intrusion Detection Systems
NIST	National Institute for Standards and Technology
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
RBAC	Role/Rule Based Access Control
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
SIEM	Security Incident and Event Management
SIoT	Social Internet of Things
SOC	Security Operations Center
SSL	Secure Socket Layer
TSN	Time Sensitive Networking
VPN	Virtual Private Network
WAN	Wide Area Network
WSN	Wireless Sensor Networks

attack strategy. In recent years, machine learning (ML) and deep learning (DL) methods have been investigated to enhance cybersecurity (Ozay et al., 2016; Xin et al., 2018; Wang et al., 2018). We investigate the role of threat intelligence and security analytics in IoT enabled smart grids. The standardization of the IoT and experimentation with various IoT-enabled architectures are surveyed in (Karnouskos, 2012; Hui et al., 2017; Boussard et al., 2018; Lin and Bergmann, 2016; Batamuliza, 2018; Chin et al., 2017; Fadlullah et al., 2018; Collier, 2017; Zaveri et al., 2016; Hua et al., 2014). Surveys focused on the smart grid have covered a wide range of security issues as outlined in Table 2. Our work builds on the existing body of knowledge and explores smart grid cybersecurity from emerging vulnerabilities perspective and scalability of existing security measures.

Table 2
Table of comparison of existing survey articles, journal articles, and conference publications

Principal theme surveyed	Related references	Overview of main contributions
Smart grids machine to machine communication	Bartoli et al. (2011)	Delves into standards that facilitate smart grid communications
Cyber threats in IoT, edge computing, fog computing	(Abawajy et al., 2018; Khan et al., 2017)	Familiarize the readers with a survey on the state-of-the-art IoT architectures, services, communication protocols and security requirements
IoT security, IoT security analytics, and IoT threat mitigation	(Ashraf and Habaebi, 2015; [illegible]e et al., 2017; Al[illegible] et al., 2017; Mendez Mena et al., 2018; Sha[illegible], 2018; Kouicem et al., 2018)	
IoT IDS	(Zarpelão et al., 2017; Wang et al., 2006)	Provide an extensive insight into routing protocols supported by the IoT operating systems and other concepts that play a critical role in sustaining IoT setups
IoT routing	Zikria et al. (2018)	
IoT resource constrained nature	[illegible] et al. (201[illegible])	
SIoT, IoT D2D	(N[illegible] et al., 2014; Militano et al., 2017)	
Renewable energy resources, wind energy, low carbon energy sources	(Das et al., 2018; Brown et al., 2012; Ippolito et al., 2014; Schachter and Mancarella, 2016; Zhang et al., 2017b; Reka and Dragicevic, 2018)	A survey on energy control systems, future of energy delivery, and how traditional power grids are being transformed into smart grids
ICS, SCADA, critical infrastructure	(Dacier et al., 2014; Cherdantseva et al., 2016; Alcaraz et al., 2011; Alcaraz and Lopez, 2014)	Investigate secure SCADA and ICS framework for the protection of critical infrastructure
CPS attacks and countermeasures	(Xiang et al., 2017; Liu et al., 2015; Srivastava et al., 2018; Wadhawan et al., 2018; Wang et al., 2016a; Zhang and Sankar, 2016)	Comprehensive survey of solutions in the context of smart grids and collaborative convergence of smart grids with IoT
Cybersecurity in smart grids	(Sun et al., 2018; Wang and Lu, 2013; Leszczyna, 2018a; Zhang et al., 2017a; Komninos et al., 2014; Deng et al., 2017; Yan et al., 2012; Jokar et al., 2012; Leszczyna, 2018b; Nardelli and Kuhnlenz, 2018; Colak et al., 2016; Bekara, 2014; Ciavarella et al., 2016; Koundinya et al., 2016; Dalipi and Yayilgan, 2016)	Security requirements, standardization current security trends in smart grids; explore security issues, challenges and countermeasures
Smart cities, smart homes	(Khatoun and Zeadally, 2017; Alavi et al., 2018; Minoli et al., 2017; Talari et al., 2017)	An insight into security requirements in smart cities and smart homes
Impact of attacks on smart grids	Shafie et al. (2018)	Impact of passive and active security attacks on smart grids
Data sharing in smart grids and data driven security in smart grids	(Hur, 2013; Tan et al., 2017)	Effective data driven approaches for next-generation security in smart grids
IoT enabled smart grids	(Karnouskos, 2012; Hui et al., 2017; Boussard et al., 2018; Lin and Bergmann, 2016; Batamuliza, 2018; Chin et al., 2017; Fadlullah et al., 2018; Collier, 2017; Zaveri et al., 2016; Hua et al., 2014)	Treat smart grids as a subset of the state-of-the-art IoT, comprising of smart meters, sensors/ home appliances, and so forth

(continued on next page)

Table 2 (*continued*)

Principal theme surveyed	Related references	Overview of main contributions
False data injection attacks in smart grids	(Hao et al., 2015; Liu and Li, 2017; Kim and Poor, 2011; Liang et al., 2017)	A review in achieving secure and authentic communication in smart grids as an indispensable requirement
Key based, certificate-based security and key management systems in smart grids	(Saxena and Grijalva, 2017; Benmalek et al., 2018; Wan et al., 2014; Tsai and Lo, 2016; Xia and Wang, 2012; Abreu et al., 2018)	An argument that key based authentication techniques may be inadequate for a smart grid setting, lacking an integral solution for secure communication between smart meters and the ICT infrastructure
Smart-metering security, phasor measurement unit (PMU)	(Fan et al., 2015; Koo et al., 2017; Han et al., 2018)	Discuss why it is essential to secure smart meters
Machine learning techniques for attack detection in smart grids	(Ozay et al., 2016; Jindal et al., 2016), (Zou et al., 2018; Xin et al., 2018; Wang et al., 2018)	Introduce the state-of-the-art application and adoption of machine learning and deep learning methods for cybersecurity against APTs in smart grids
Authentication, authorization, and accounting (AAA) smart grids	Liu et al. (2014)	AAA for critical domains, this paper addresses a critical multi-dimensional research issue in smart grids
HAN, NAN, FAN	(Xiao et al., 2013b; McCary and Xiao, 2014; Lee et al., 2016)	Investigate smart grid applications from feasibility point of view and evaluate their performance
NIST standards and recommendations for smart grid cybersecurity	Anonymous (2013)	Emphasize privacy considerations and privacy preservation for smart grid information security
Blockchain for tamperproof cyber security	(Khan and Salah, 2018; Malomo et al., 2018)	An introduction to Blockchain security approach for next generation cybersecurity
Attacks, vulnerabilities, and ransomware in IoT and smart grids	(Chakhchoukh and Ishii, 2015; Chen et al., 2018; Esnaola et al., 2016; Sou et al., 2013; Luo et al., 2018; Zhu et al., 20[illegible])	Surveys on the idea of threat actors, [illegible]ted cyberattacks, and [illegible] malicious attackers target [illegible]mation exchange with ransomwares
Advanced persistent threats (APTs), command and control (CnC), and cyber kill-chain	(Wang et al., 2016b; Auty, 2015; Sood and Enbody, 2013; Lemay et al., 2018; Chen et al., 2018)	Survey APTs and command and control, and cyber kill-chain

1.4. Article organization

The rest of the paper is structured as follows: The next section defines key terms and technologies in IoT-enabled smart grids. The section provides an overview of the emergence, evolution and adoption of smart grids and their role in sustaining IoT and smart cities (Alavi et al., 2018). The section then outlines the components and various vulnerabilities in smart grids that serve as potential ingress points for attackers and malicious intruders (Wade et al., 2010). Data transfer to and from cloud storage are discussed in this section (Singh et al., 2016). Section 3 discusses the specialized protocols designed to facilitate IoT device-to-device (D2D) and machine-to-machine (M2M) communication (Bartoli et al., 2011). The section then identifies privacy concerns in smart grids and attack motives in smart grids (Jokar et al., 2012).

Section 4 classifies attackers as threat actors based on the sophistication of attacks they can launch. We then discuss how advanced persistent threats (APT) and malware can be hideously injected into smart grids (Wang et al., 2016b; Auty, 2015; Sood and Enbody, 2013; Lemay et al., 2018; Chen et al., 2018). We also analyze whether and how the traditional network security measures pertaining to confidentiality, integrity, and availability (CIA) triad scale to smart grids (Sou et al., 2013; Zhu et al., 2015). We discuss current trends that aim to detect, tackle, and mitigate APTs tunneled within legitimate communication protocols. The section concludes with a comparison of security requirements in traditional computing systems, supervisory control and data acquisition systems (SCADA), industrial control systems (ICS), and smart grids (Zhang et al., 2017a). This comparison outlines how threat actors continue to evolve and gain necessary expertise and skillset to break into secure systems, and how smart grids' security demands differ from those of traditional computing systems, SCADA and ICS (Fan et al., 2013; Abdrabou, 2016; Schuurman et al., 2012; Bou-Harb et al., 2013; Le et al., 2017).

Section 5 describes attacks and intrusions as systematic and organized processes, known as cyber kill-chain, executed by motivated, skilled, and perseverant threat actors (Wang et al., 2016a). We also summarize that while intruding smart grids, the attackers need not follow all the steps of cyber-kill chain, thus making it challenging to detect intrusions and threats that go unnoticed, without raising suspicion (Auty, 2015). The section concludes with an introduction to diamond intrusion detection model that describes intrusions as a four-pronged process and countermeasures to mitigate the cyber kill-chain (Batamuliza, 2018).

Section 6 introduces novel attack surfaces introduced in smart grids and IoT by using cutting edge communication technologies (Saxena and Grijalva, 2017). We discuss how time sensitive networking (TSN) is a critical communication principle in smart grids and how it is potentially exploited by threat actors to introduce time as an attack vector (Pop et al., 2016; Zhao et al., 2018). Finally, the paper concludes by identifying [illegible] research directions in tackling security pitfalls and emerging threats in IoT in general and smart grids in particular (Barreto et al, 2014; [illegible]ar et al., 2017).

2. Internet of Things-enabled smart grids

2.1. Fog computing and cloud computing

In the context of IoT and smart grids, fog and cloud computing facilitate computation, data processing, communication and storage near the edge devices (Abawajy et al., 2018). Cloud computing is a communication and data storage architecture central to the rise of IoT that allows data storage on distributed storage systems instead of central storage (Butun et al., 2014). Fog computing enables faster data communication in IoT. Fog and cloud computing offer mechanisms to create massively scalable and flexible self-organizing networks, centered on automation and data-driven control facilitated by wireless connectivity (Butun et al., 2014). Cloud computing enables IoT applications by integrating connectivity with other field devices while fog computing provides a gateway between the IoT sensor layer and the data storage-based cloud computing layer (Mendez Mena et al., 2018). Fog computing offers the following advantages in IoT:

- Geographically distributed mobile applications (Ashraf and Habaebi, 2015)
- Low latency (Ge et al., 2017)
- Distributed control systems (Ban et al., 2016)

Fig. 5 depicts multitude of applications enabled by IoT, which utilize cloud and edge computing to speed up data communication and reduce overhead. Cloud computing provides shared resources for storage, analysis and information processing (He et al., 2018). Though some IoT networks include a firewall between the cloud and the IoT node, yet with increased connectivity, security remains a crucial aspect both from technology as well as communication standpoint (Schuurman et al.,

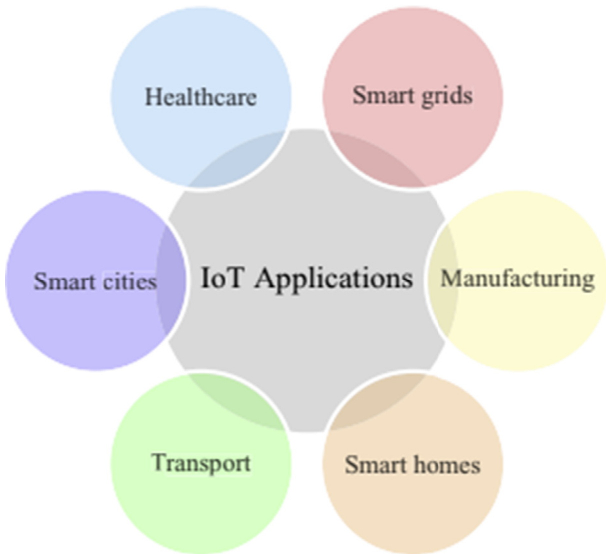


Fig. 5. Cloud computing, fog, and edge computing in the IoT, IoT applications, and IoT-enabled smart grids (Subashini and Kavitha, 2011).

2012). Ensuring secure connectivity is vital in IoT ecosystem as the threat actors continue to evolve. Infrastructure monitoring complements firewalls, authentication mechanisms as well as identity and data security measures such as automated payload encryption (Saxena and Grijalva, 2017). These methods provide data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies (Esnaola et al., 2016). However, even with these mechanisms in place, IoT networks remain vulnerable to multiple attacks aimed to disrupt the network. For this reason, another line of defense known as intrusion detection systems (IDS) is needed to detect attackers and intruders (Chen et al., 2018).

2.2. Advantages of smart grids in powering smart infrastructure and emergence of threat vectors

Smart grids offer following advantages by adopting advanced networking and wireless communication in electric grids (Dacier et al., 2014).

- *Reduction in Carbon emissions:* Although carbon rich energy sources such as coal and gas lead to major electricity generation, they also contribute to global warming (Schachter and Mancarella, 2016). Lower carbon-content energy sources such as nuclear and renewables are subject to uncertain availability (Brown et al., 2012). Wind and solar energy inconsistently vary with geography, are climatically restrained and are susceptible to insufficient availability at crucial times (Zhang et al., 2017b). Smart grids provide a greener solution to inconsistent availability of resources (Leszczyna, 2018a).
- *Sustainable electricity generation:* International summits on global warming and environmental safety have raised notable calls for bringing about a fundamental change in the way electricity is consumed (Brown et al., 2012), as well as to allay low consumer engagement in electricity industry (Abdrabou, 2016).
- *Electricity consumption:* Residential cooling/heating and transportation industry are seen as the prevalent energy consumers. With emergence of electric vehicles, smart cities, smart homes, intelligent street lights and illumination, electricity is likely the highest priority option to serve the futuristic energy needs (Wade et al., 2010). Moreover, digitized devices communicating with the smart grid also serve as novel threat vectors (Hossain et al., 2012).
- *Decentralized energy generation:* Smart grids locate the energy generating sources close to the location of energy consumption (Mendez Mena et al., 2018), leading to prosumers, defined as consumers who can generate electricity. Prosumers present a noteworthy challenge to existing generation-distribution structure, in moving on from one-way power transmission to two-way transmission (Luo et al., 2018).

2.3. Components of smart grids

The smart grid communication and data transfer is classified into information data and operation data (Bartoli et al., 2011). Information data consist of meter readings, consumer bills, power prices, tagging and trending, and consumers' geographical location. The operational data consists of real-time current and voltage levels in a network, capacitor banks, fault locations and energy storage values. (Bartoli et al., 2011; Dacier et al., 2014). The core and peripheral technologies that make smart grids are composed of various intelligent devices listed below:

- *Active Network Management (ANM)*: Provides innovative means to record individual device power usage patterns, voltage controls, fluctuation levels, and dependable data transfer between substations and the grid components [44. However, ANM introduces the risk of sniffing, data falsification, spoofing, and replay attacks (Guo et al., 2015).
- *Automatic Voltage Control (AVC)*: Voltage fluctuations and demand variations bring unnecessary device failures. The AVC is a set of controls that monitor voltage levels inside preset breaking points, and enable smart grids to self-balance sub-stations, self-heal networks, and network optimization (Dacier et al., 2014). From security viewpoint, AVC is susceptible to tampering by malicious third parties (Alakhchoukh and Ishii, 2015).
- *Dynamic Line Rating (DLR)*: The DLR minimizes transmission line losses by letting smart grid consumers and power generators to determine transmission line capacity and apply line ratings in real time, securely (Liu et al., 2014). It also reduces network congestion, increases context-awareness, and reduces greenhouse emissions (Dacier et al., 2014).
- *Intelligent Electronic Device (IED)*: This type of devices provide microprocessor-based control of power system equipment, substation protection, and power quality recording and measurement capability (Bartoli et al., 2011). Device authentication, encryption, authentication, and freshness of communication messages pose cybersecurity threats to smart grids (Das et al., 2018).
- *Phasor Measurement Unit (PMU) and Reactive Power Compensation*: The PMU measures electrical waves on an electricity grid using time synchronization to obtain real-time measurements of multiple remote measurement points on the grid (Fan et al., 2015).
- *Distributed Generation (DG)*: DG is power generation at the consumers' end, by the consumers. DG framework cuts down transmission cost around 30% (Anonymous, 2013).
- *Dynamic Demand (DD)*: In conventional electric technology, electrical appliances such as refrigerators and cooling/heating systems do not make time-specific requests on the control system. The DD framework is a technique for ensuring appropriate power supply upon request (Jindal et al., 2016).
- *Smart meters*: Smart meters provide end users as well as the smart grid control centers with essential analytics and an in-depth perspective of device power consumption pattern (Anonymous, 2013). Intelligent autonomous devices optimize electricity usage by receiving constant and accurate feedback on usage patterns from the smart meter and advanced metering infrastructure (AMI) to offer: real-time pricing, time-of-use pricing, critical peak pricing (Dacier et al., 2014).
- *Smart Appliances*: Smart appliances are cyber-physical systems (CPS) capable of monitoring power consumption in real-time. The end-user devices are more easily accessible for exploits than core smart grid

network as they are perimeter devices, it remains a key subject to examine the cybersecurity impacts of this type of two-way communication on the smart grid infrastructure (Dacier et al., 2014).
- *Smart Homes*: Smart homes represent the human side of the smart grid, redefining the relationship between energy, utilities, and consumers that modernize the role of energy in daily lives (Dacier et al., 2014). A smart home fitted with smart meter co-ordinates manageable energy-use for advanced mobile and cyber-physical appliances (Anonymous, 2013).

Fig. 6 depicts various distributed networks such as home area network (HAN), neighbor area network (NAN), field area network (FAN), wide area network (WAN) responsible for role-based data transfer between utility data centers, substations and smart meters (Xiao et al., 2013b; McCary and Xiao, 2014; Lee et al., 2016). The core components of smart grids such as the automated network management (ANM), advanced metering infrastructure (AMI), peripheral devices etc. are installed in specific networks (Lee et al., 2016). A communication scenario between smart grid components is elaborately depicted in Fig. 7.

2.4. Summary and insights

In this section, we have comprehensively surveyed various advantages offered by smart grids, and the potential of threats and vulnerabilities induced alongside these opportunities. The section explored how smart grids are supported by the IoT (Sou et al., 2013). The section further highlights that smart grids are no more a distant dream, evolving into a digital power distribution system consisting of smart meters, sensors and other devices that can communicate reliably, capture data at every point of the grid, and make better decisions (Saputro et al., 2012). It was revealed that the two-way communications in smart grids lead to massive data exchange, requiring strong measures against spoofing, data tampering, and authentication attacks (Sharma and Saini, 2017).

3. Internet of things: key-terms and supporting technologies

3.1. Emerging and proprietary protocols and standards for smart devices

The underlying communication protocols in smart networks execute data transfer in three phases:

- Collection phase: This phase is the fundamental IoT data collection stage where inbuilt, embedded and mounted sensors accumulate contextual data from the surroundings to gather information about the physical conditions (Lakhchoukh and Ishii, 2015). Sensors coupled with short distance wireless communication capabilities work at restricted information rates and short separations, with limited memory, and low bandwidth utilization (Ban et al., 2016). Due to these qualities, accumulation stage is also known as low power and lossy networks (LLN) (Barreto et al., 2014).
- Transmission phase: In this phase the data gathered in the previous stage are transmitted to neighboring nodes, users and applications which are transformed into meaningful information in the subsequent phase (Chen et al., 2018). This phase generally uses TCP/IP and related protocols such as Ethernet and Wi-Fi. Default gateways are an important component during this stage to enable transmission compatibility between TCP/IP and LLN protocols (Barreto et al., 2014). Other standard industrial communication protocols include OLE for Process Control - Unified Architecture (OPC UA), International Society of Automation (ISA) 100.11a, and Highway Addressable Remote Transducer Protocol (HART). A discussion on security in these protocols is beyond the scope of this survey and interested readers may refer to (Fan et al., 2013; Abdrabou, 2016; Qiu et al., 2011; Cavalieri and Regalbuto, 2016; Yoo and Shon, 2016) for

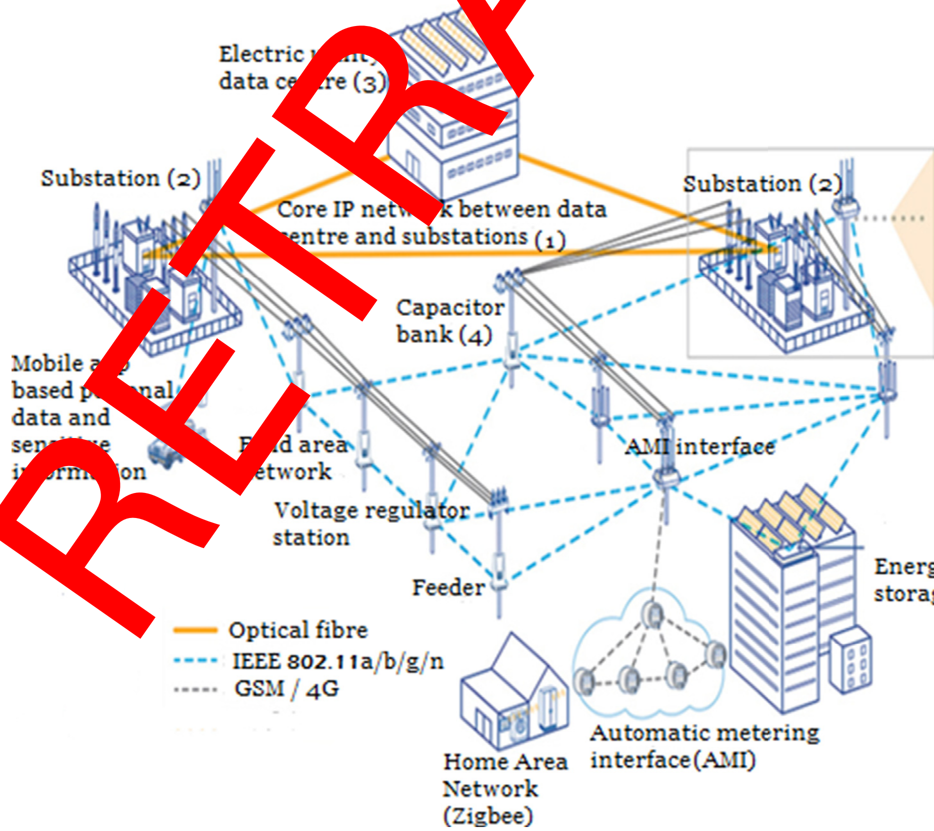


Fig. 6. Smart grid: An Information and Communication (ICT) enabled electricity generation, transmission and distribution network consisting of information data and operation data (Dacier et al., 2014).

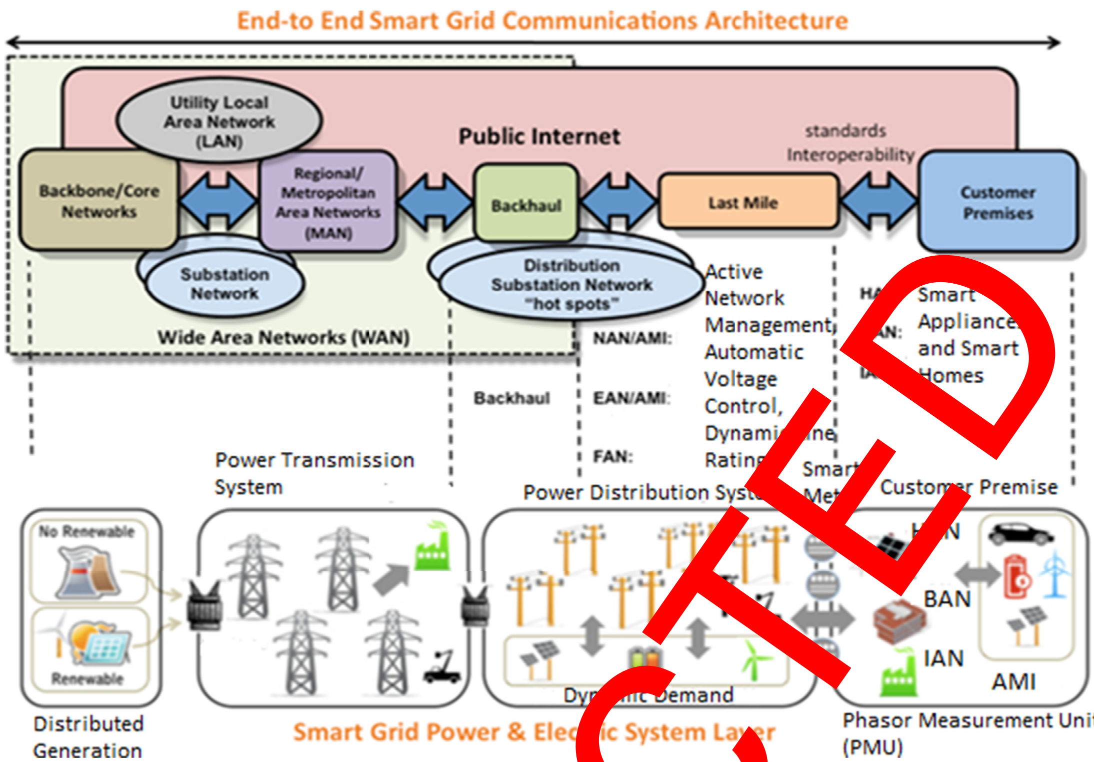


Fig. 7. Internet based communication between components of smart grid (Schuurman et al., 2012).

detailed surveys on smart grid and industrial communication protocols.

- Processing, management and utilization phase: In this phase, accumulated data are processed by applications to obtain information about the node's physical space. This phase calls for multi-platform requirements encouraging the coordination and correspondence between various physical IoT nodes (Ashraf and Habaebi, 2015). Two widely used protocols at this stage are the IEEE 802.15.4 and Internet protocol version 6 (IPv6) over low-power wireless personal area networks (6LoWPAN), which facilitate interoperability between IPv6 and LLN nodes (Schachter and Mancarella, 2016). Yet, a compatible passage between the IPv6 and LLN based networks is important that is provided by a default gateway (Barreto et al., 2014; Hur, 2013).

3.2. Threat visibility and intrusion detection in smart applications, smart grids, and IoT

An attempt made by an unauthorized user to gain access into a protected network is known as an intrusion. Intrusion detection systems (IDS) are used to detect unauthorized access to assets and resources (Pop et al., 2016). The IDS are network security components that monitor access attempts made to gain access to trusted devices and legitimate applications (Dacier et al., 2014; Alcaraz and Lopez, 2014). Along with detecting malicious users through continuous asset tracking, IDS also offer advanced human machine interface (HMI) alerting the network administrators and security professionals when a malicious activity is detected (Khanna et al., 2016). The confidentiality, integrity and availability (CIA) of time-critical information exchange in IoT, smart grids, and other mission critical infrastructure is enhanced with strategic placement of IDS (Saputro and Akkaya, 2015). However, due to a large number of connected devices in IoT, and IoT-enabled smart grid networks, the traditional IDS techniques to alert the human users each time an alert occurs does not scale well (Sou et al., 2013). Furthermore, considering the number of false positives generated by IDS will make it difficult to holistically monitor information flow. This section investigates various intrusion detection techniques that have been applied to the IoT architecture and analyses their scalability to the IoT-enabled smart grid landscape (Collier, 2017; Zaveri et al., 2016). The IDS for IoT differ from IDS for traditional systems primarily in the following aspects:

- The IoT nodes such as Internet enabled smart grids, smart watch, smart pen, smart health-care, and smart vehicles are miniaturized electronic devices with significantly low computing power compared to traditional computing devices such as smart phones, laptops, mainframes, desktops and tablets (Ban et al., 2016).
- The IoT nodes have a small payload and make use of line of sight wireless communication such as Bluetooth low energy (BLE), ZigBee, IEEE 802.15.4, and near field communication (NFC) which have a small bandwidth suitable for limited data transmission. The traditional computing devices utilize communication architectures that consume larger bandwidth than IoT nodes can process (Qiu et al., 2011).
- Smart grids, critical infrastructure, and the IoT nodes use new and specifically defined communication protocols such as low-power wireless personal area networks (LoWPAN) and IPv6 whereas the traditional computing systems are based on TCP/IP protocol stack that is centered around the standard Ethernet-based data exchange (Schachter and Mancarella, 2016). The IDS need to be compatible among various protocols to allow seamless integration. Different and novel protocols incorporate unforeseen and original vulnerabilities and place cutting-edge demands on IDS (Ban et al., 2016).
- The traditional computing systems rely on IDS that alert users when a malicious activity is detected (Kim and Tong, 2013). While such methodology is appropriate in the context of such devices, smart grids are more susceptible to malicious access due to increased attack surfaces (Cherdantseva et al., 2016; Alcaraz et al., 2011). The number of alerts generate by IDS is generally too large for a user to be alerted each time (Shafie et al., 2018). To combat this limitation, intelligent IDS combined with capabilities for intrusion prevention and discarding of false positives are required (Tan et al., 2017).
- Traditional computing systems are protected by techniques such as virtual private network (VPN) encryption, VPN credentials,

embedded systems, cryptography, trusted infrastructures and predictive maintenance, where each component contributes to defense-in-depth architecture (Hao et al., 2015; Liu and Li, 2017). Low computing power in embedded IDS calls for additional computing resources to avoid risking a bottleneck through overutilization of the available resources (Karnouskos, 2012).

- Smart nodes such as smart homes, smart cities, end-user IoT devices use sensors to gather context information to make intelligent decisions (Kang et al., 2017). The need to secure the gathered information intensifies for vital applications such as power plants, smart grids, and transportation systems where security exploits result in terrible consequences for cities and nations (Alavi et al., 2018). To secure these nodes, a strategic placement of network-based IDS at various ingress and egress points is critical (Tan et al., 2017).

The connected nature of smart ecosystem such as IoT and smart grids is such that in order to safeguard these networks, unauthorized intruders must be detected within the node constraints of each type of device at the earliest possible stage (Komninos et al., 2014), thus leading to different security requirements (Deng et al., 2017).

3.3. Intrusion detection systems: types, architectures, recent advances, and applicability in IoT-enabled smart grids

Intrusion detection systems safeguard traditional networks and information systems from unauthorized access (Koo et al., 2017). The IDS monitor the operations of a host or a network, alerting the system administrator when a security violation pertaining to logins and access controls is detected. However, applicability of IDS to IoT networks for mitigating threats and challenges to privacy, traffic analysis, and denial of service (DoS) is still an active area of research (Chakhchoukh and Ishii, 2015; Chen et al., 2018; He et al., 2017). Malicious activities place high demand on wireless sensor network (WSN) node's energy consumption and diminish the sensor lifetime (Brown et al., 2012). The IDS can be divided into the following four types:

- Anomaly based IDS: These types of IDS are based on aberrance identification strategy centered on a benchmark system activity (Dacier et al., 2014) that describes acclaimed, legitimate, and acknowledged baseline system behavior, figured out over time and specified by system administrators. Whenever events and network practices outside those predefined models are detected, the analytics and baselining system alerts the users (Abdrabou, 2016). This technique, though computationally expensive, allows the IDS to scale as the vulnerable activities grow and call for increased caution (Zarpelão et al., 2017). A drawback of anomaly-based IDS is a high number of false positives. With a large number of communicating devices in smart grids and IoT, it is difficult to characterize and set baseline standards. As network protocols continuously evolve and dynamically adapt to their context, the IDS investigations must also be constructed likewise. The biggest challenge for IDS in smart grids and IoT is to evolve into frameworks that can recognize new robotized worms and malware (Hao et al., 2015).
- Signature based IDS: These types of IDS consist of identifications that include organized and legitimate movement of network traffic (Hur, 2013). This identification technique used by these IDS is simple to create and is efficient at detecting and recognizing known threats and malicious activities (Alaba et al., 2017). A signature is comprised of specific strings that describe misuse embedded in a payload. The instances created by signature-based IDS allow for matching to be performed exceptionally rapidly with respect to present day frameworks (Abdrabou, 2016). However, signature-based IDS identify only the known attacks; a novel threat cannot be distinguished (Ban et al., 2016). They also generate false positives as they are dependent upon general expressions and string matching. They fail to identify a large number of attacks activated by a human threat actor or a worm induced self-modifying behavior (Abdrabou, 2016). Identification is further muddled when pernicious attackers hide their scripts behind payload encoders and encrypted information channels (Alaba et al., 2017).
- Specification based IDS: Specification-based IDS use manually specified behavioral determination to identify attacks and have been widely recommended for IoT node abuse identification. The IDS usually return true positives from claiming known attacks combined with an ability to recognize novel attacks (Fan et al., 2013). However, the success of these IDS is based on human expertise that builds specification-based identification framework through continuous experiments and studying widely available network activity datasets (Guo et al., 2016). Since threats attacks as deviations from normal behaviors, the possibility to recognize formerly obscure attack patterns is enhanced (Fan et al., 2013).
- Hybrid IDS: These IDS amalgamate the separate frameworks that are distinctive to anomaly and signature-based IDS (Brown et al., 2012). These IDS utilize signature databases to trigger alarms once an alternate activity is detected. Hybrid IDS provide the benefits of different approaches to overcome the inconsistency of updating and detecting new threats.

Due to infrastructural differences between conventional computing systems, IoT, and smart grids, suitable prevention and protection strategies need to be devised for IoT network as well as IoT-enabled smart grids (Guo et al., 2016). These networks continue grow in sophistication through:

- Cloning of IoT devices to appear as legitimate nodes
- Maliciously substituting IoT nodes with rouge devices
- Firmware and operating system (OS) replacement
- Modification of security configurations and policies

In (Karnouskos, 2012), the authors proposed to use IDS at the edge of the network to filter internal and external traffic to detect attacks and mitigate unwanted consequences. In (Koo et al., 2017), the authors argue that as embedded IDS in IoT have limited processing capacities, they are not used to implementing security policies. The IDS as network edge devices (NED) facilitate trust center between the external Internet, internal network and the internodal communication. The IoT architecture needs to dedicate resources to allow self-reorganizing of the nodes upon discarding compromised hubs (Hao et al., 2015). The feasibility of this technique was in question as discarding a hub would break the communication link and lead to service disruptions (Fan et al., 2015). The user reaction to service disruptions is subjective, although in sensitive applications the chain of connected devices must not be broken, initiating further investigation into effective IDS strategies. A re-authentication mechanism was proposed by (Chakhchoukh and Ishii, 2015) where the discarded hub could re-enter the IoT network using a digital signature and public key infrastructure (PKI) based verification. This would organize the IoT hub as it was before a node is discarded (Wade et al., 2010).

A modified technique employed disseminated aberrance identification which resulted in a time-consuming process for mobile-agent-based identification. The IDS agents employed in dynamic, mobile and versatile IoT hubs were restricted to detect intrusions based on nearby-node information and neighborhood identification. Authors in (Ippolito et al., 2014) proposed a novel light weight IDS for resource constrained sensor nodes to detect denial of service (DoS) attacks. These IDS are deployed as centralized modules causing saving of energy on sensor nodes (Bartoli et al., 2011). Due to centralized nature of IDS location, adding location information of nodes enhanced system efficiency for detecting wormhole attacks with smaller overhead and with high true positive rate (Butun et al., 2014). This method accounted for a relatively low and fixed number of TCP packets and analyses for attack detection (Bartoli et al., 2011). The method gives high detection rate in resource constrained environments but the low number of analyzed packets undermined the high detection rates (Ban et al., 2016). With the emerging threat vectors in IoT and smart grids, the detection system itself needs to be immune to DoS attacks (Khan and Salah, 2018). A DoS attack flooding the target with traffic can influence the network connections rendering it inaccessible to legitimate users (Ban et al., 2016). The threat actors target the web servers of high-profile organizations such as banking, commerce and media companies through DoS attacks on IoT nodes (Das et al., 2018). Authors in (Hao et al., 2015) proposed the following five-step IDS operation strategy to detect tunneled worms in legitimate 6LoWPAN network traffic:

- *Package signature checking:* Every IoT node uses the central IoT publisher's public key to verify digital signatures on all packets received, dropping invalid packages. This helps to identifies rogue peers and evil twins (Hao et al., 2015).
- *Caching:* Packets moving through nodes cached in local storage are susceptible to duplication of transmitted data allowing several legitimate nodes to respond to data (Hao et al., 2015).
- *Tracking neighbors:* IoT nodes must be aware of physical or logical identification such as IPv6 addresses of other nodes, perhaps through human collaboration (Hao et al., 2015). This serves to transmit and receive authentic packets (Barreto et al., 2014).
- *Package updating:* Packets protected by digital signatures are appended with refreshed timestamps in order to invalidate old packets. Nodes are also expected to discard a data packet once it becomes stale, i.e. the timestamp exceeds the set limit (Hao et al., 2015).
- *Content advertising:* Nodes inform the neighbors about the cached and recently transmitted data in a separate packet (Hao et al., 2015).

The authors in (Fan et al., 2015) advance the packet authentication mechanism by proposing triple factor authentication where data gathered by the sensors are passed through visualization and statistical analysis phase. Correlation of gathered IDS data with other data sources helps decipher a number of security vulnerabilities that allow a local attacker to gain unauthorized access to data (He et al., [illegible]). The IDS clear the data and store intrusion time and place in real time for corresponding nodes (Fan et al., 2015). However, the resource constrained sensors embedded in IoT nodes grow less effective to determine intrusion as the battery-driven micro controller sensor nodes are limited in terms of computational power and memory size (Ban et al., 2016). When equipped with sensors and wireless communication capabilities, nodes often lack protection due to their hardware limitations such as energy consumption, detection rates, network reliability and latency in detecting different routing attacks such as sinkhole attacks, wormhole attacks, and selective-forwarding attacks (Chakhchoukh and Ishii, 2015).

3.4. Privacy concerns in smart grids

Smart grids are increasingly being perceived as green and environmental-friendly solutions for power generation that would enable the end-users to generate power locally through environmental-friendly means such as solar cells and wind turbines (Esnaola et al., 2016). Any excess power generated could be uploaded back into the grid. This would also enable users to reduce electricity consumption and the electricity bill by selling their excess power. While these are legitimate benefits of smart grid, there is still a paucity of information on the steps taken to protect and secure the personal information collected through the smart grid (Zarpelão et al., 2017). Given the ability of local users to upload power, fears arise that malicious hackers could break into the grid's communications network through smart components such as meters and appliances to destabilize the grid. Security mechanisms need to be supplemented with security policies to exercise control over the manner in which a user's personal information is accessed, collected, used and disclosed, safeguarding both the privacy as well as the environment (Chen et al., 2018).

The modern smart grids and digitized substations require high availability, performance, real-time communication (sub Nano-second time-synchronization) networks and service availability to handle ever-growing massive data (Momoh, 2012). Innovative communication, utility wide Area networks (WAN), wireless mesh networks (WMN), automated substation and distribution station, mobile workforce are restrained by the issues related to data privacy, encryption, message security and access control (Chen et al., 2018). For example, the connection of a neighbor area network (NAN) or home area network (HAN) client to a nearby substation's IEDs needs network access control (NAC), identification and admission control, and authentication management policies in place (Ashraf and Habaebi, 2015). Pole top equipment, smart meters, scheduled maintenance and runtime availability of backups require time references from synchro phasors (Chen et al., 2018). Certificate revocation, key management and network timestamp verification generate large quantities of data logs for security incident and event management (SIEM) and valuation (Al-rimy et al., 2018). Fig. 8 depicts various smart grid domains that are susceptible to cyberattacks (Jokar et al., 2012).

3.5. Attack motives in smart grids

Smart devices scattered in physically insecure locations and public wireless communication channels used to access smart grids lead to increased user engagement as well as introduce new security challenges (Mendez Mena et al., 2018). Malicious users might try to gain access to critical AMI, HAN, NAN and FAN for the following nefarious purposes:

- *Reduce the bill:* Users might want to evade paying for exact usage hours by reducing bills (Butun et al., 2014).
- *Fool the billing system and change meter readings:* This is done to mislead the control center to make erroneous decisions (Wade et al., 2010)
- *Exploit the knowledge of the power system configurations to simulate smart grids:* This knowledge can be later used to launch bigger attacks, or to place rouge smart grids into network. The rouge smart grids lure unsuspecting users to log in, divulge sensitive personal information, and get manipulated in despicable ways (Butun et al., 2014).
- *Increase the cost for energy distribution:* This type of attack may be motivated by competitors trying to bring other distributors into disrepute and hence losing customer base (Wade et al., 2010).
- *Gain acceptance in the hacker community*: A class of attackers known as script-kiddies break into systems to gain popularity as hackers and to impress friends (Lim and Taeihagh, 2018).
- *Personal revenge:* An attacker may intend to blackout specific houses, companies, employer establishments and public areas for personal reasons. A more serious impact is tampering with victim's smart meter data to ridiculously high usage readings (Han and Xiao, 2016).

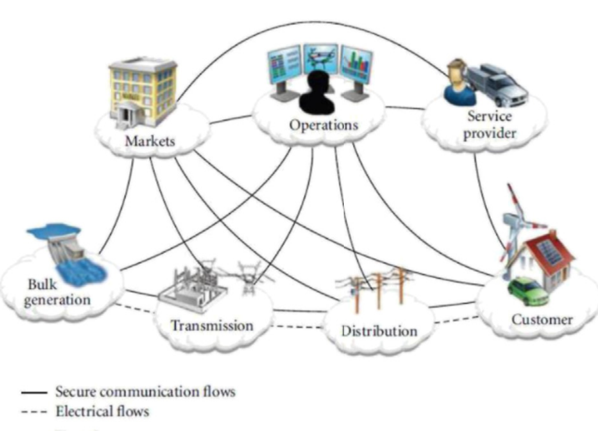


Fig. 8. Smart grid domains (Jokar et al., 2012).

- *Stop production:* Motivated by financial gains from corporates and foreign governments, hackers might just want to bring smart grid infrastructure to a standstill (Lim and Taeihagh, 2018).
- *Ill-will and nuclear competition among nations:* As smart grids are accessible across geographical boundaries, cyberwarfare is set to gain momentum with the advent of smart grids (Shaukat et al., 2018).

In AMI, smart meters, and smart grids, attacks compromise integrity and availability of data (Saputro and Akkaya, 2015). In smart grids, the attacks on data integrity and availability are categorized as network attacks, system compromise and DoS attacks (Nitti et al., 2014). These attacks lead to operational failures, misleading operational decisions, loss of synchronization of critical smart grid equipment, or large-scale blackout (Xiang et al., 2017). Smart grid core network comprises of real-time operational tools such as state estimators, energy management systems, and data gatherers, which are reported to be highly vulnerable to cyberattacks by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (Liang et al., 2017).

Smart meters and advanced communication networks have also been utilized in SCADA and ICS (Xiang et al., 2017). However, the communication architecture of smart grids is more vulnerable to cyberattacks due to increased entry points into the network (Momoh, 2012). As an attacker needs prior information about the system to launch an attack, advanced IDS provide a network analysis tool to detect the presence of the attacker in the network while trying to gather system information (Berger and Iniewski, 2012). However, their computational power requirements need more attention in the low-voltage power distribution scenario. Moreover, with encryption and evasion techniques such as tunneling, an intruder can inject false data in a way that the system is unable to detect (Hossain et al., 2012). Smart meters deployed across a utility's coverage area communicate with the utility and with other devices via a wireless network that offers multiple ways to intrude into the equipment (Kim and Tong, 2013). Also, network security features such as firewalls can be bypassed by attackers having a sufficient degree of intent, motivation and expertise (Schachter and Mancarella, 2016).

3.6. Centralized and distributed IDS placement in IoT-enabled smart grids

The low-end consumer devices in a modern grid serve as a potential target for hackers by virtue of the technical ease of exploiting vulnerabilities that need less computational power to break into the system (Liu and Li, 2017). A single compromised node renders an entire network vulnerable (Kim and Poor, 2011)- (Liang et al., 2017). A sophisticated attacker possesses the ability to launch attacks against proprietary nodes through botnets (a collection of large number of infected machines with significant computational capabilities and processing power) and to automate the attacks to exploit the vulnerabilities (Hao et al., 2015).

With the advent of open source systems, the attack mechanisms can be freely posted on the Internet for others with mechanisms published for the knowledge of other attackers (Saxena and Grijalva, 2017). Various open source tools can be used to detect the presence of smart devices (Kang et al., 2017). Often, these devices are mass produced, each unit is essentially identical and one vulnerability can be used to further exploit hundreds, thousands or millions of connected devices (Khan and Salah, 2018). Furthermore, threats increase in severity as small and inexpensive smart devices and their software solutions lack memory banks and computing power of traditional devices (Ban et al., 2016). These nodes utilize embedded lightweight real-time operating systems (RTOS) that lack a pre-integrated and inbuilt security solution to evade cyber-attacks (Chen et al., 2018), leading to various attack surfaces increasing the probability of being under an undetected attack (Srivastava et al, 2018).

Smart nodes are equipped with logging and reporting capabilities to detect when a hacker tries to probe or penetrate a network (Fan et al., 2013). Network security and physical security of these mission critical systems are the underlying factors that model the quality of their services. Security by obscurity (Chen et al., 2018) is safe in only until a threat actor makes a determined effort to discover vulnerabilities in a device (Militano et al., 2017). The IDS reduce the workload on other security mechanisms such as role-based access control (RBAC), firewalls, access control lists (ACLs), and cryptography and encryption techniques (Butun et al., 2014). These techniques enhance privacy and trust among users and devices and enforce current security and privacy policies (Han et al., 2018). In this placement strategy, IDS need to be optimized in order to be energy aware in resource-constrained environments (Ban et al., 2016). Intrusion detection strategies applicable to different networks, layers and phases of operation in smart grids are summarized in Table 3. This includes data generated from remote commands, troubleshooting and diagnostic data, and consumer data. The table mentions different security policies such as authentication policies, confidentiality policies, non-repudiation policies, access control and integrity policies in order of precedence required to safeguard the consumer data, remote login data, or component diagnostics data (Komninos et al., 2014), (Deng et al., 2017).

3.7. Summary and insights

This section emphasizes the fact that cybersecurity must stay at the forefront of electric grid digitalization. In the current era of constantly changing and accessible technology, attacks are considerably easier to launch and harder to detect. The section explored intrusion detection and threat visibility procedures used in IoT, and their scalability to smart grids. Due to emerging automation and communication protocols in smart grids, wrapping one security layer upon another in a layered security architecture reduces areas for potential intrusion. The section highlighted various motives that lead to cyber threats, and the need for means to provide end-to-end security. The section concludes that in order to achieve effective cyber hygiene, user privacy and resilience to

Table 3
Intrusion detection strategies applicable at various networks, layers and phases of smart grids.

Intrusion detection strategies	Requirement, deployment techniques, and applicability in IoT-enabled smart grids
Intrusion detection by design (Butun et al., 2014)	• Integrated IDS manufacture (Butun et al., 2014) • IDS within system components (Ippolito et al., 2014) • Designing IDS from scratch with embedded security solutions (Hao et al., 2015)
Intrusion detection in-depth (Hao et al., 2015)	• Acknowledges that any IoT and smart grid network, however secure by design, is eventually breakable (Ashraf and Habaebi, 2015) • Emphasizes the need for layered security (Ban et al., 2016) • Layered IDS to detect, deter, delay intrusion attempts (Abdrabou, 2016) • Access control intrusion detection, host intrusion detection systems (HIDS) (Nitti et al., 2014) • Firewall based intrusion detection for bidirectional data communication (Nitti et al., 2014) • Profiling traffic and pattern, network intrusion detection systems (NIDS) (Nitti et al., 2014)
Intrusion detection for end-to-end communication devices (Hao et al., 2015)	• Large number of intelligent intrusion detection sensors placed in local proximity of smart grid devices (Saputro and Akkaya, 2015) • Proximity of users (Melese and Avadhani, 2016) • Remote login requirements (Huang and Yuan, 2015) • Whitelisting rather than blacklisting (Wade et al., 2010)

cyberattacks, smart grids must be equipped with built-in, multi-layered security to protect data at rest and in transmission.

4. Threats, vulnerabilities, exploits, and threat vectors in IoT-Enabled smart-grids

An individual or a group of individuals responsible for a malicious incident that negatively impacts the security posture of a network is called a threat actor (Fan et al., 2013). Threat actors are categorized based on a combination of skill level, type of activity within the network, and their pursuing motivations. There are threat actors who perform the attack simply for their own amusement, or just to see if it can be done; whereas some threat actors may have a social agenda or a strong political motivation (Karnouskos, 2012). The IoT ecosystem provides them with an opportunity to break into unauthorized networks with various malicious intents (Abdrabou, 2016). The IDS provide mechanism to alert security administrators about such hidden malicious attempts (Chakhchoukh and Ishii, 2015). In the following, we list the major threat actors in smart grid and IoT:

- *Script Kiddies*: It is defined as an incompetent individual who employs readymade scripts to alternate a specific application or operation (Saxena and Grijalva, 2017). Script kiddies often penetrate into IoT networks for fun or other nefarious purposes such as to deface a website and ruin a network operation. Their operation strategies are restricted to hunt and misuse easy-to-find shortcomings and vulnerabilities in IoT nodes and accessible networks, often haphazardly (E-ISAC White paper, 2016). These actions are often an attempt to awe their companions or to gain popularity on computer-enthusiast groups (Saxena and Grijalva, 2017). However, these threat actors are not viewed as hazardous exploiters of security lapses in the IoT networks (E-ISAC White paper, 2016).
- *Hacktivists*: Unlike script kiddies, these are advanced threat actors compared to script kiddies and possess strong fundamentals in programming and network exploitation (Koo et al., 2017). The activities undertaken by hacktivists often encompass various political convictions, motivations and issues. Hacktivists propose activism in a form that is malicious and destructive to IoT architecture undermining the IoT network security (Saxena and Grijalva, 2017). Hacktivists contemplate downing or intruding a network as an opportunity to cause political persuasion (E-ISAC White paper, 2016). Moreover, these threat actors have unintended consequences where security threats and risks are often disguised but destructive (Mendez Mena et al., 2018).
- *Organized Cyber-criminals*: Although the script kiddies and hacktivists can execute a handful of network security exploits using commonly available reconnaissance and attack tools, they often lack financial and infrastructural resources to carry out large scale DoS attacks and other severe exploits (Mendez Mena et al., 2018). To cause advanced cybercrimes, assemblies of human beings possessing advanced technical skills combined with financial resources have begun to emerge (Koo et al., 2017). These threat actors are termed as organized cyber criminals and their key feature is access to large botnets and other malicious infrastructure with state-of-the-art computational speeds. These threat actors often work in exchange of financial gains and provide third party network exploitation services. Malicious security activities arise from foul placement and execution of refined and specialized technical abilities (E-ISAC White paper, 2016)- (Koo et al., 2017). These threat actors do possess skills required to script and build complex ransomware frameworks aimed to intrude IoT networks at a stupendous scale (Mendez Mena et al., 2018). They are adept at using malicious packet tunneling programs to spread malware to steals sensitive, confidential and top-secret information from a contaminated node (Koo et al., 2017).
- *Nation state sponsored threat*: Nation-state hackers progressively focus on administration institutions, offices, nuclear storehouses and SCADA systems of an enemy nation and aim to bring down as much critical networks as possible to wreak havoc through the Internet (Mendez Mena et al., 2018). Furthermore, Nation-state sponsored threats span a wide number of organizations capable of complex threat scripting and publicizing techniques capable of intruding critical operations to spill secret data (Saxena and Grijalva, 2017). With growing cyberwarfare collaborating with the advent of increased connectivity through IoT, dangers for digital attacks from nation-states add a powerful dynamic to the cyber threat landscape (Koo et al., 2017). Nation-state actors progressively focus on administration institutions, offices, nuclear storehouses, communications infrastructure, AMI, PMU, and distributed energy resources (DER) (Fan et al., 2015; H[illegible] et al., 2018).

4.1. Challenges posed by cybercriminals and threat actors to smart grids and IoT infrastructure

While the Internet revolution and wireless communication lead to the emergence of smart grid, they also present the biggest challenge to smart grids (Fan et al., 2013). Secure communication strategies such as encryption tunneling, virtual private networks (VPN) offer both secure communication as well as means for attackers to obfuscate communications and remain obscure (Melese and Avadhani, 2016). Some prevalent smart grid cyber security challenges are outlined below:

- *Evolving face of cybercriminals and threat actors*: Modern day cybercriminals are highly motivated professionals, often well-funded, far more patient, perseverant and persistent, rather than being mere opportunists breaking into softer targets and shying away from secure encounters (Hui et al., 2017). The attacks on networks are becoming more organized and prevalent (Ma et al., 2018).
- *Advanced attackers and the state of today's intrusions*: The emergence of Advanced Persistent Threats (APTs) has revolutionized the way networks and smart systems are attacked (Zhang et al., 2017b). APTs enable the attack as well as the attacker to remain obscure and undetected while displaying unprecedented resiliency, intelligence and patience to intrude, exploit and eventually disrupt the network (Zhu et al., 2018). Whereas no universal and single security solution is capable of mitigating these threats, the next-generation IDS and firewalls offer unique visibility, control and integration of threat-prevention disciplines needed to find and stop both known and unknown threats (Hui et al., 2017).

4.2. Advanced persistent threats (APTs)

The APTs refer to a highly sophisticated, well-planned, and methodical cyberattack that begins with doing reconnaissance on an intended victim (Komninos et al., 2014). APTs are usually backed by well-funded criminal groups, military organizations or government agencies to gain proprietary data, classified information or similar data for profit or to damage national security (Deng et al., 2017). As APTs do not leave tangible, suspecting or detectable trace, they are capable of a wide range of cyber-assaults that differ from the usual attack methodologies (Yan et al., 2012). Cybersecurity risk modeling exemplified by the theory of cyber kill-chain summarizes a lack of formalized threat modeling and evaluation practices that scale vertically and horizontally (Jokar et al., 2012). Vertical scaling concerns with embedded device safety and horizontal scaling harps on precise cybersecurity goals embodied by smart grids. An example of one such cyber attack is the December 2015 Ukrainian electric grid disruption (E-ISAC White paper, 2016) that led to wide-scale power outage. In summary, APT enters a network and inserts malware. The network, compromised and vulnerable to a severe breach, is probed for additional network access and vulnerabilities (Leszczyna, 2018b). The malware collects data on a staging server, then exfiltrates the data off the network under the control of a threat actor. The APT continues the data breach bypassing the traditional cyber security measures such as defense-in-depth, firewalls and antivirus (Leszczyna, 2018b). Interested readers may refer to (Wang et al., 2016b; Auty, 2015; Sood and Enbody, 2013; Lemay et al., 2018; Chen et al., 2018; Mell et al., 2006) for detailed description and further insights on APTs and existing countermeasures.

4.3. The role of malware in advanced persistent threats

Malware is malicious software or a piece of code that typically damages, disables, takes control of, or steals information from a computer system. Malware includes botnets, viruses, worms, Trojan horses, logic bombs, rootkits, backdoors, spyware, and adware (Wang and Lu, 2013). The rise of propelled malware is reshaping the risk scene, outpacing universal anti-malware methodologies in the process, forcing researchers to reassess how networks are safeguarded (Wan et al., 2014). Bots are individual contaminated machines leading to the more extensive collection called botnets. Attacks and malware originating from these bots are notoriously troublesome for conventional antivirus/anti-malware to identify (Fan et al., 2015). Key characteristics of malware undetectable by traditional intrusion detection systems are: distributed and fault tolerant (Fan et al., 2015), multifunctional (Koo et al., 2017), persistent and intelligent (Hao et al., 2015), targeted intrusion (Militano et al., 2017), DDoS and botnets (Sha et al., 2018), and malware-as-a-service (Zhang et al., 2017b).

4.4. Life cycle of an advanced attack

As opposed to a conventional attack against a high-value server or network asset, today's attackers utilize a patient, multi-step methodology that blends exploits and malware avoidance (Hao et al., 2015). Attacks against smart grids lure an end-user to click a contaminated connection or link, usually through social applications. The remote individual then tries further exploits to gain root entry on the smart grid network (Qiu et al., 2011). The malware enters the network, permitting the attacker to further expand on the inner network, escalating privileges on the contaminated machine, or creating unapproved accounts (Zhang et al., 2017b). Malware is progressively altered to avoid detection, providing the remote attacker with an instrument for persistence and communication to summon further control. The four steps in the advanced malware deployment are infection, persistence, communication, and command and control (Zhang et al., 2017). These steps are briefly described as follows:

- *Infection:* The smart grid network consists of the core network, HAN, NAN, FAN and the end-user peripheral component network (Ge et al., 2017). Infecting the core smart grid network usually begins by contaminating the end-user or peripheral IoT device through a social aspect such as getting users to click links to a phishing e-mail, luring them through an interpersonal interaction site, or through a malware-affected free download (Guo et al., 2016). With IoT devices such as refrigerators used to send a tweet, or a smartwatch used to keep track of health and same devices used to log in to smart grids to pay utility bills, the infection is not solely reliant on email (Wang et al., 2016a). Social media, webmail, message boards, microblogging platforms are some of the evolving threat vectors (Wang et al., 2016a).
- *Persistence* (Wang and Lu, 2013)*:* Once an initial machine is infected, the attackers' ability to hold on to the decent footing in the network defines the flexibility and survivability of the attack (Wang and Lu, 2013). Rootkits allow persistence, introducing attackers to having privileged root-level access rights in the compromised nodes (Cardenas et al., 2014).
- *Communication* (Barreto et al., 2014)*:* it defines the attackers' ability to deliver malware to the components of the smart grids such as smart meters, AMI, or electricity distribution network (Barreto et al., 2014). A single step to bring down a smart grid is infeasible and the attackers need to gradually escalate their grip on the smart gird (Hashemi-Dezaki et al., 2015). Communication is also used to extricate stolen information from a target framework. This attack and intrusions related communication is stealthy and obfuscated, transmitted without raising suspicion on the network (Leszczyna, 2018a). Following techniques are used to achieve successful communication from to infect devices:
  - ➢ *Encryption:* Proprietary encryption is used to prepare malware such as ransomwares, which require a high degree of reverse engineering to decrypt (Barreto et al., 2014). The malware can execute its objective well before the malware is reverse engineered (Leszczyna, 2018a).
  - ➢ *Circumvention:* Logins to protected networks via proxies and remote access login tools is an example of crime-ware-as-a-service and tunnels malicious applications within other legitimate applications and protocols (Subashini and Kavitha, 2011).
  - ➢ *Port evasion:* Network anonymizers and mixers are used by attackers to port hop and tunnel over networks (Barreto et al., 2014). Botnets send command and control communication over internet relay chat (IRC) and other instant messaging apps (Auty, 2015). Encryption, encoding and obfuscation avoid detection and conceal the true motive and purpose of the malware (Sood and Enbody, 2013).
  - ➢ *Fast flux and dynamic DNS:* Gaining unauthorized access through multiple infected hosts, routing traffic over geographically diverse IP addresses to render it difficult for forensic teams to trace the origin of attacks (Subashini and Kavitha, 2011).
- *Command and control (CnC):* It uses the established communication platforms to ensure controllable, manageable, and updatable attack (Wang et al., 2016b). The CnC is accomplished through applications such as webmail, social media, P2P networks, blogs, and message boards. The CnC traffic does not raise suspicion as it is encrypted and communicated through backdoors and proxies (Auty, 2015).

Earlier, malware was delivered through e-mail attachments, whereas today, malware can be delivered to a network through many applications. File transfer applications, webmail, status updates, instant messaging, social media analytics, SIoT, microblogging, and workflow collaborations imply that the attackers are endowed with a wide range of tools and more targets to attack (Leszczyna, 2018a) (Subashini and Kavitha, 2011). The severity of impact is further compounded by the fact that most of these attacks operate in real-time and are obfuscated in nature (Leszczyna, 2018a). However, upon malware delivery, communication is the key to launch attacks (Zhao et al., 2018). Preventing a threat from communicating with remote control centers can help to neutralize attacks. With data analytics enabled IoT devices, numerous opportunities exist to detect and correlate malware as an extensible framework rather than a functional payload (Leszczyna, 2018a). Table 4 summarizes the ingress points through which malware can be potentially introduced in the smart grid computing, telecommunication, and the electricity generation and distribution sector. Ageing infrastructure, network modernization, adaptive self-healing, outages, remote authentication, as well as communication with peripheral devices are a few challenges that need to be enhanced with secure mechanisms to detect and prevent malware propagation.

4.5. The threefold threat: the convergence of social media, secure socket layer & APTs in IoT and smart grids (Wan et al., 2014)

In order to maximize the availability and user reachability, a large number of modern IoT devices and applications bypass conventional firewalls. This facilitates injecting malware and invisible threats into the IoT node which remain unperceived and uncontrolled (Komninos et al., 2014). Such evasive applications and CPS make it easy for an attacker's traffic to blend in with normal user traffic and traverse the network

Table 4
Malware threats in smart grid components SUCH as computing infrastructure, telecommunication and electricity generation, transmission and distribution (Leszczyna, 2018a; Zhao et al., 2018).

Malware threats in smart grid computing infrastructure (Subashini and Kavitha, 2011)	Malware threats in smart grid telecommunication (Subashini and Kavitha, 2011)	Malware threats in smart grid electric sector (Subashini and Kavitha, 2011)
Use case vulnerabilities taken from published documents from standard agencies (Barreto et al., 2014)	Use cases pertaining to reliable delivery of electricity (Khanna et al., 2016)	Electric smart grid use-cases (Subashini and Kavitha, 2011)
Smart grids with utility network modernization (Leszczyna, 2018a)	Advanced sensor-based PMUs (Khanna et al., 2016)	HAN device provisioning (Ge et al., 2017)
Aging infrastructure (Subashini and Kavitha, 2011)	Automatic outage reporting (Barreto et al., 2014)	HAN pricing and consumer opt-out (Ge et al., 2017)
Challenges related to delay, clock generation and distribution (Koo et al., 2017)	Proprietary communication protocols between HAN, NAN, FAN and peripheral devices (Ge et al., 2017)	In-field programming of smart meter and firmware upgrade (Momoh, 2012)
Complex interactive capabilities in self-adaptive and self-healing smart grid networks (Barreto et al., 2014)	Ethernet and cellular connectivity, layer2 and layer3 services (Subashini and Kavitha, 2011)	Smart meter remote connect-disconnect (Leszczyna, 2018a)

without suspicion. Traditional IDS, IPS and firewalls rely on ports to ascertain which mechanism to use for detection and analysis, and which signatures to analyze and look out for (Subashini and Kavitha, 2011). Malwares primarily rely on secure socket layer (SSL) encryption and obfuscation to hide malicious content as well as CnC traffic. As SSL is default social media and social connectivity protocol used for music streaming, multimedia content browsing is a fertile ground for SIoT malware delivery (Guo et al., 2016; Wan et al., 2014).

Tunneling is another technology that renders IDS and firewalls largely ineffective in smart grids. (Karnouskos, 2012) Tunneling allows attackers to hide malicious traffic inside legitimate applications and protocols, peer to peer applications and encrypted traffic ([illegible] et al., 2013). Disguised communication leads malicious packets and APTs to circumvent traditional IDS and firewalls, thus evading perimeter security (Schachter and Mancarella, 2016). Installing proxy servers on infected host device allows the bots to hide their communication by establishing anonymous networks to hide traceability (Momoh, 2012). Anonymity tools such as Tor, Himachi, UltraSurf are purpose built to evade network security measures. Applications are updated on monthly and weekly basis to circumvent, deliver and hide (Li et al., 2012). Social media is a well-established hub for social engineering malware infection, and CnC (Wan et al., 2014).

IoT devices in a smart grid network provide access through single-sign-on and federated social networking, web-based e-mail, instant messaging, web-based file transfers, message boards, and micro-blogging (Wan et al., 2014). Consequently, these applications are targeted by attackers as they provide easy uncontrolled access to the weakest link in network security, the end user. Gaining the trust of an unsuspecting user leads to links, scripts, ads, and images, all of which can be used to exploit a larger smart grid network. In order to improve user privacy, these applications use SSL encryption as default protection for traffic (Sun et al., 2018). This move to SSL has ironically transformed to security flaw by encrypting the channels used by malware to attack the network (Hui et al., 2017). Instead of trying to hide behind a circumventor application that may draw unwanted attention, the attackers can hide within the SSL connection between the end-user and application (Nitti et al., 2014).

Earlier, malware was categorized by the ability to replicate and spread to a wide number of host, infecting more machines in less time (Sun et al., 2018). Advanced malware is more qualitative, intelligent and networked, with the attacker having the ability to remotely control the malware one deployed on the targets. Deadly attacks can be launched from a single infected machine rather than from a multitude of infected hosts (Hui et al., 2017). Polymorphism is an approach used by malware to avoid IDS signatures through regular mutation. Some malware applications have sections of code that serve no purpose other than to change the malware signature (Hui et al., 2017).

4.6. *Emerging threat vectors in smart grids*

Conventional perimeter security solutions classify, allow, and block traffic based on the port and protocol in operation. Evasive and dynamic threats bounce to an unexpected port, avoid detection and gain access to the network (Zhu et al., 2018).

4.6.1. *Limitations of firewalls and proxies in smart grids*

Firewalls provide first line of defense against threats by segmenting a network into various zones ([illegible] et al., 2018). Their port-centric design is inadequate to detect and prevent evasive malware. Anti-malware capabilities incorporated into firewalls, known as unified threat management (UTM) result in poor accuracy and performance degradation (Hui et al., 2017). The IDS and IPS based on signature matching apply to specific traffic based on ports and the APTs utilizing standard ports or uncommon ports remain undetected (Nitti et al., 2014). Proxies safeguard against a specific set of applications and protocols (Boussard et al., 2018). Proxies mimic applications that lack updates and lack knowledge of mechanisms used by attackers to hide protocols within protocols to tunnel malicious traffic. In addition, proxies usually investigate only a portion of traffic leading to performance issues (Al-rimy et al., 2018).

4.6.2. *Network and host-based approaches in smart grids*

Network-level intelligence complements end point security measures. Smart grid consists of various purpose-specific networks, IoT based networks, and numerous smart appliances (Ge et al., 2017). Smart grid network security must render the ability to detect the presence of APTs on the network, including the network of bots and botnets (Boussard et al., 2018).

4.6.3. *Integrating multi-disciplinary solutions to provide next generation security in smart grids*

Preventing APTs and advanced obfuscated cyberattacks in smart grid calls for an integrated, multi-disciplinary approach to detect malicious traffic and correlate events from various segments of the smart grid network (Ozay et al., 2016). In addition to legacy port-based firewalls, IPS and proxies, many segregated security approaches such as web-content filtering, antivirus gateways, application specific solutions, and anti-spam detection mechanisms exist (Jindal et al., 2016). However, monitoring ingress points and data correlation is not straightforward, as the context between events might be inadequate due to vastness of smart grid networks (Hashemi-Dezaki et al., 2015). Also, above mentioned security solutions are limited to their backgrounds and application domains. As a result, more security appliances do not lead to more secure network.

To counter the limitations mentioned in the previous paragraph, rather than focusing on ports, protocols and IP addresses, whitelisting users is considered a strong way to monitor who exactly has access to what part of the network (Alaba et al., 2017). Complexity of smart grid network and inconsistency of security solutions can be detrimental to smart grid security enabling the following attacks: social engineering attacks (Alaba et al., 2017), network and routing attacks (Al-rimy et al., 2018), password attacks (Alaba et al., 2017), application attacks (Alaba et al., 2017), physical sabotage (Alaba et al., 2017), asset theft (Al-rimy et al., 2018), privilege escalation (Abdrabou, 2016), or exploiting ZigBee/Bluetooth devices (Liu and Li, 2017). Table 5 builds on the malware

RETRACTED

Table 5
Scope of emerging threat vectors in smart grid ICT (Schuurman et al., 2012).

Threat Vectors Leading to Data Theft (Alaba et al., 2017)	Threat Vectors Leading to Data Distortion (Al-rimy et al., 2018)	Threat Vectors Leading to Tampering with ICT Infrastructure (Abdrabou, 2016)	Threat Vectors Leading to Data Loss (Alaba et al., 2017)
Smart meter tampering to steal electricity (Wade et al., 2010)	Analysis of device usage patterns (Ashraf and Habaebi, 2015)	Fraud monitoring and data reconciliation between smart meters and access points (Wan et al., 2014)	Smart grid control center (Guo et al., 2016)
Multiple passwords (Alaba et al., 2017)	Privacy by design and privacy by default (Khan and Salah, 2018)	Wireless Personal Area Network (WPAN) with integrated wireless meters (Leszczyna, 2018a)	Data generated by SCADA and AMI network (Wade et al., 2010)
Layered security and (Alaba et al., 2017)	Identification of relevant risks (Schachter and Mancarella, 2016)	Two-way communication and distributed connectivity (Hui et al., 2017)	Data explosion from peripheral devices (Zhang et al., 2017b)
Remote meter access attempts (Nitti et al., 2014)	Severity and likelihood of identified risks (Wang et al., 2016a)	Rogue device identification and physical security to protect access points (Xiang et al., 2017)	Trusted communication from anywhere, anyone, any device (Zhao et al., 2018)
Port access attempts (Dacier et al., 2014)	Safeguarding confidentiality and security of transmitted data (Singh et al., 2016)	Large geographical smart grid territory extending from remote generation sites to congested urban distribution centers (Zhao et al., 2018)	Threat intelligence, security analytics, and disaster recovery (Zhao et al., 2018)

ingress points introduced in Table 6 and highlights intrusion detection, intrusion prevention, and data theft prevention requirements in smart grid infrastructure. The above-mentioned requirements have been classified into data theft prevention, data distortion prevention, communication infrastructure prevention, and data loss prevention.

Increasing popularity of alternate and renewable energy sources such as solar and wind energy summons the utilities to adapt these distributed energy sources in smart grids (Das et al., 2018). Smart grid communications rely on applications where IP-based, packet-switched networks form the backbone system providing interoperability, enhancing grid security as well as rendering provisions for control and automation (Wang et al., 2006). Based on the threats posed by various threat actors, the smart grid threat landscape identifies the attack vectors based on (Chakhchoukh and Ishii, 2015) as device property (Das et al., 2018), location (Das et al., 2018), strategy (Das et al., 2018), access levels (Wang et al., 2006), information [illegible] levels (Huang and Yuan, 2015), and communication protocols (Huang and Yuan, 2015).

However, this threat vector analysis classifies the attacks based on their origin and the network characteristics under target. The analysis does not mention specific types of IDS that can detect these attacks (Alaba et al., 2017). As Internet revolution and technical innovation span energy sectors, the need for next generation security requirements to protect smart grids from APTs and malware becomes pronounced. Whereas adoption of SSL to protect user applications and communications leads to a moderate improvement in privacy for the users, it also makes a network far more vulnerable to organized attacks, lost data, and compromise (Butun et al., 2014).

Networks lack the ability to enforce security on SSL encrypted communications and are unaware of potentially malicious traffic (Hao et al., 2015). Offering a clear path for malware to get in and out of smart grid network, social media applications on end-user cyber-physical devices continue to be the preferred point of entry to smart grid networks (Luo et al., 2018). Applications based on single sign-on capabilities inadvertently make it easier for malware to remain hidden by default use of SSL to protect user communications, highlighting important challenge for security (Ge et al., 2017). As cybercriminals thrive on the ability to merge malicious content within approved, legitimate, and seemingly normal traffic, substantial and deep network visibility is crucial to protect smart grid assets and user privacy (Alaba et al., 2017).

Next-generation firewalls (NGF) are envisioned as a potent security measure against APTs in smart grids, they provide reliable and comprehensive visibility of network traffic irrespective of ports and obfuscation techniques used (Al-rimy et al., 2018). Threats need to communicate with remote control centers in order to execute their actions on the objective. The NGFs detect this communication to control cyberattacks and to mitigate the threats they pose (Alaba et al., 2017). They provide an integrated approach to threat prevention with coordination across multiple security disciplines such as application identity, malware and exploit detection, intrusion prevention, file type controls, and content inspection ([illegible] et al., 2015). They interpret and classify potentially complex stream of traffic at the application level (Koo et al., 2017). NGFs are embedded with the ability to progressively scan traffic and peel back the traffic layers to examine protocols running within protocols, until the [illegible] underlying application is identified. This ability to identify complex, hidden and obfuscated traffic is crucial to detect unique CnC traffic (Wade et al., 2010). In addition, they impart due diligence and consideration to constantly detect and avert cyberattacks capable of jeopardizing an entire nation's critical and top-secret infrastructure (McCary and Xiao, 2014). Secure connectivity drives smart grid efficiency, resiliency, and delivers next generation services to a wide array [illegible] and mobile customer base (Sha et al., 2018).

Summary and insights

This investigated into the cybersecurity challenges that emerge as a result of smart grids and utilities implementing advanced communication networks. Although these networks enable many benefits of the AMI systems, the attackers have also harvested vulnerabilities in these communication and data transfer mechanisms. Individuals and organizations exploit networks through multi-tiered attacks, adopting strategies such as ransomware, credential harvesting, crypto malware and beyond. Proactive malware management is used to address the issues concerning malware leveraging a range of security options such as firewalls, multi-layer encryption, asymmetric encryption, key management technologies, and access control for smart endpoints. In a wide-spread threat scenario ranging from unsophisticated hackers to nefarious governments, best practices and approaches to address security concerns need to be complemented with network design to keep attackers at bay. Increased digitalization of critical infrastructure and an endless web of interconnected devices in SCADA and ICS leads to exponentially higher risks in smart grids. The section explored the scalability of effective SCADA and ICS security strategies, to smart grids, and how new communication protocols and technologies call for better coordination, real time network visibility, anomaly detection, smart grid network monitoring, incident response, AI-enabled correlation, and rapid remediation.

5. Attack procedure (cyber kill-chain) and security analytics in IoT

The notion of connected IP-enabled D2D and M2M communication has transitioned from being buzzwords to real-world devices currently in advanced phases of deployment and utilization (Bartoli et al., 2011). Yet, the widespread adoption of D2D and M2M communication between devices connected through the cloud is heavily reliant on how these devices address the implicit security and privacy concerns (Zhang et al., 2017a). Newer cybersecurity challenges in IoT are frequently reported by security agencies such as the United States Department of Defense (DoD),

Table 6
Comparison of prominent ICT security features and requirements in traditional computing systems, ICS/SCADA systems and smart grids (Koo et al., 2017).

Prominent ICT security features (Fan et al., 2015)	Traditional computing systems	ICS/SCADA	Smart grids
Security through obscurity (Butun et al., 2014)	Security through obscurity widely used in conventional computing and enterprise infrastructure (Wang and Lu, 2013)	Security through obscurity of device locations (Wade et al., 2010)	Size and scalability renders security through obscurity infeasible (Ozay et al., 2016)
Ports and protocols for communication and encryption purposes (Hui et al., 2017)	Well defined ports and protocols, some proprietary protocols widely used (Hur, 2013)	Proprietary protocols (Hui et al., 2017)	Evolving revisions, regulations, and standards (Wang and Lu, 2013)
Proprietary protocols and documented universal protocols (Zarpelão et al., 2017)	Documented protocols, Request for Comments (RFC) available from the Internet Engineering Task Force (IETF) (Chakhchoukh and Ishii, 2015)	Undocumented protocols and little documented protocols widely used (Chakhchoukh and Ishii, 2015)	Low power protocols such as ZigBee, Bluetooth low energy (BLE), proprietary undocumented protocols (Zhang et al., 2017a)
Remote access (Liu et al., 2015)	Remote access a key feature and operational requirement (Liu et al., 2015)	Remote access not widely adopted to enhance privacy (Liu et al., 2015)	Remote access a key feature, primarily for remote troubleshooting and maintenance (Liu et al., 2015)
Encryption (Zhang et al., 2017a)	Encryption widely recommended (Zhang et al., 2017a)	Encrypted end-to-end communications (Zhang et al., 2017a)	Encryption recommended but encrypted and obfuscated malware a security threat (Zhang et al., 2017a)
Network segmentation (Lin and Bergmann, 2016)	Network segmentation and logical separation required for operational feasibility and network management (Lin and Bergmann, 2016)	Physically separated/isolated locations (Lin and Bergmann, 2016)	Network isolation and segmentation less encouraged due to millions of IoT devices, user whitelisting preferred (Lin and Bergmann, 2016)
In-built security measures (Srivastava et al., 2018)	Cybersecurity is considered a separate subject, a necessary add-on, although applications increasingly being designed with consideration to security (Srivastava et al., 2018)	No inherent cybersecurity measures built-in, mostly applied as add-ons (Srivastava et al, 2018)	Built-in cybersecurity measures mandatory (Ma et al., 2018)
Legacy devices (Mendez Mena et al., 2018)	Legacy devices used in some cases (Mendez Mena et al., 2018)	Legacy devices are insecure (Mendez Mena et al., 2018)	Integrated and interoperable array of legacy and modern devices (Mendez Mena et al., 2018)
Backups and data-retention (Kim and Poor, 2011)	Frequent scheduled backups (Kim and Poor, 2011)	Less frequent scheduled backups (Kim and Poor, 2011)	Frequent scheduled backups (Kim and Poor, 2011)
Time synchronization (Alcaraz et al., 2011)	Network Time Protocol (NTP) used for time synchronization, albeit not at sub micro second scale as in smart grids (Alcaraz et al., 2011)	Time synchr[illegible]red, obtained through undocumented proprietary protocols, [illegible] dependent on applications and machine[illegible]et al., 2011)	Stringent time synchronization requirements (Alcaraz et al., 2011)
Physical security (Brown et al., 2012)	Securing Desktops, mobile devices, applications and log-on (Brown et al., 2012)	Securing factory and production devices (Brown et al., 2012)	Securing smart meters, smart appliances, home energy controllers (Brown et al., 2012)

RETRACTED

National Institute for Standards and Technology (NIST), National Institute for Standards and Technology Interagency Report (NISTIR), the North American Electric Reliability Corporation Critical Infrastructure Prevention (NERC-CIP), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Open Web Application Security Project (OWASP) (Liang et al., 2017; Nitti et al., [illegible]; Cherdantseva et al., 2016). Smart grid cybersecurity is broadly defined as the "*set of operational and logical techniques that inhibit cyber actions a[illegible] to partly or completely jeopardize the CIA triad of smart grid by disrupting the underlying information systems, security policies, acceptable use policies, privacy policies and data transfer over covert and overt communication channels*" (Benmalek et al., 2018). An unauthorized access into secure smart grid ingress points is termed as intrusion that endangers [illegible] the data at rest as well as the data in transit (Han et al., [illegible]).

Reportedly, attackers and threat actors follow a series of steps when attempting to intrude a network or [illegible]. The series of steps executed in to systematically gain unauthorized access to a cyber-physical framework is known as the cyber kill-chain (E-ISAC White paper, 2016). Ref (Al-rimy et al., 2018). emphasizes the significance of intelligence-driven defenses that provide an understanding of the adversarial tactics. The study conducted by (Tsai and Lo, 2016) has examined the network-based as well as endpoint-driven resistance methodology using next generation firewalls (NGF) (Huang and Yuan, 2015). This research has raised many interesting questions emphasizing the need to foresee the vulnerabilities that might be exploited upon intrusion (Tsai and Lo, 2016). Assessments reveal that threat actors do not stay in their starting work areas but extend to other core areas of the smart grid upon gaining entry (Schachter and Mancarella, 2016). Any data as small as the electricity usage patterns for an hour might reveal personally identifiable information about the users (Ippolito et al., 2014). The cyberattacks have transitioned from being one-dimensional DoS attacks, worms, and viruses to being an integrated framework comprising Internet, computational power and intelligence, teamwork as well as economic and commercial gains (Kim and Tong, 2013). Cyber kill-chain for smart grids helps develop an operationally relevant model for security planning, policymaking, research, and execution (E-ISAC White paper, 2016).

5.1. Multi-stage cyber-attacks in smart grids

Smart grids' control, manage, generate, transmit, distribute, utilize, and recycle operations are layered architecture, with IoT and end-users at the edge of the layer, while control and manage operations exist at deeper, core layers (Wade et al., 2010). A single act of network penetration is inadequate for threat actors to achieve their goal to disrupt operation reliability of smart grids (Ozay et al., 2016). Cyber kill-chain defines a step-by-step multistage cyberattack that exploits the interdependence between the ICT network, peripheral IoT device network, HAN, NAN and the power grid network (Hansen and Shenoi, 2017). The next step of these dynamically interrelated attack steps unfolds through the completion of the previous step. A multistage attack through APTs and advanced malware enters smart grids through the cyber network and poses threat to impact both the cyber as well as the core physical system (Liang et al., 2017). A failure in confidentiality, integrity, and availability (CIA) at any stage of the smart grid, however minor in timescale and magnitude of effect, can have a cascading effect of devastating failures (Liu et al., 2015).

The multistage cyberattacks usually begin with identifying a system to target. The attacker then strives to learn more about the associated networks, communication infrastructure, protocols and operating systems used at various IT and IoT devices to discern vulnerabilities in the target (Wang et al., 2006). This step is known as reconnaissance (Wang et al., 2006). This is followed by designing customized malware or APT and injecting them through specific delivery points ascertained during reconnaissance (Anonymous, 2013). This lets the attacker intrude the network and it depends on the attackers' technical expertise to remain obfuscated and undetected in the network for as long as possible, without raising suspicion (Esnaola et al., 2016). Privilege escalation, implanting malicious applications and programs to execute nefarious outcomes, steal critical information, exfiltrate sensitive data to outside data centers and cloud storage are the closing stages of a successful attack (Wang et al., 2006).

Fig. 9 depicts a layered reference model known as cyber kill-chain framework to comprehend the cyberattacks and related risks in IoT and cyber-physical systems (Zhu et al, 2018). Smart grids are a potential target for intrusion, and the smart grid cybersecurity model proposed by NIST emphasizes the need to apply security requirements at every segment of the grid (E-ISAC White paper, 2016). The Lockheed-Martin cyber kill-chain outlines a wide array of intrusion-based threats. In this context, risk to smart grids is defined as the likelihood of an unwanted outcome resulting from an intrusion and vulnerabilities are defined as exploitable weaknesses (E-ISAC White paper, 2016). Traditional approaches in IT security such as cryptographic primitives and firewalls are either incompatible, outright inapplicable, insufficiently scalable, or inadequate to secure cyber-physical systems such as smart grids. Safety requirements, vulnerability aspects and functional interdependencies of smart grids are becoming increasingly sophisticated as well as prone to multistage cyberattacks. The ability to compromise core physical equipment such as distribution and generation control centers usually begins with unsuspecting and trivial attacks on peripheral devices and user networks (Cherdantseva et al, 2016). Threats and attacks aimed with the objective to disable power generation, tamper with distribution equipment, or render transmission unavailable at critical times are evolving over time, with cybercriminals becoming increasingly patient, perseverant and technologically empowered (Khan et al., 2017). The seven steps to describe a cyberattack proposed in Lockheed-Martin cyber kill-chain are elucidated below.

- Reconnaissance: The initial step in cyber-attack where the intruder simply engages with the target network or device to assess hazards and identify vulnerabilities (Khanna et al., 2016). Based on the findings, the attacker develops operational goals and attack methodologies to exploit vulnerabilities and gain a deep entry into the target system (Ayar et al., 2017). Attacks such as phishing, spear phishing, and whaling are also executed at this step to gather further information about the target and ascertain some potential points of entry into the network (E-ISAC White paper, 2016).
- Weaponization: Today, interaction within and through digitized data is evolving and more data are consumed than ever before through smart phones, smart objects, computers, IoT and SIoT (Cardenas et al., 2014). Weaponization is a crucial cyber-attack step where the attacker transmits misleading and manipulated data packets to a receiver. These packets are usually in form of a web link, application, image, or certain lucrative posts that take advantage of psychosocial characteristics of human users. Consequently, user may be prompted to unsuspectingly click otherwise dangerous links, out of fear of losing out or fear of missing out (Saxena and Grijalva, 2017). Malwares and APTs are two most commonly used weaponized payloads in smart grid and IoT environments. Weaponized information is a highly skillful example of social engineering, where appealing topics and captivating information are crafted to exploit common cognitive biases and errors, just to get people click malware infected links (E-ISAC White paper, 2016).
- Delivery: The weaponized payload transmitted to the intended end-user or recipient is known as delivery. As soon as the link is clicked, or an attachment is opened, the malware or malicious packet enters the target system and propagates to further segments of a network. This provides escalated privileges to attackers and allows them to move freely in the target network (E-ISAC White paper, 2016).
- Exploitation: The malware or program code starts executing and performing the intended task on the target system or network (Saxena and Grijalva, 2017). This task could be as trivial as to deface a web page, denial of service or as devastating as sensitive data exfiltration, ransomware delivery, encryption, or modification of information (E-ISAC White paper, 2016).
- Installation: Malware is often intelligent and adaptable to locate rootkits and backdoors to provide additional entry points for intruders and attackers. This opens multiple avenues for attackers to exploit network and remain hidden (E-ISAC White paper, 2016).
- Action on Objectives: Intruder is successful to achieve the desired goal such as to deliver a ransomware, block access to legitimate users, and other malicious intentions (E-ISAC White paper, 2016).
- Command and Control (CnC): The malware and APTs frequently communicate with the remote attacker in order to receive further instructions in real-time or for the exfiltration of stolen data (E-ISAC White paper, 2016).

5.2. *Access control techniques for malicious attack and ingress prevention in smart grids*

Access control consists of authentication, accounting and authorization (AAA) to investigate and log who is endeavoring to gain access, the originating point of the endeavor, time of endeavor, access methods used to execute the endeavor and the devices targeted to intrude smart grids (Liu et al., 2015). Users trying to gain access are endowed with varying privileges and authorization, spanning from no-access, read-only, write-only and full access (Hui et al., 2017). Accounting involves post access tracking of user activities such as further log-on attempts, activities executed and time stamp of each activity (Schachter and Mancarella, 2016). Whitelisting is a positive control model that allows wanted traffic and applications instead of blocking all unwanted users and applications (Melese and Avadhani, 2016). Monitoring and restricting access control serves following outcomes: reduced attack surface (Khan and Salah, 2018), enhanced protection against cloud-based advanced malware-enabling applications such as crime ware-as-a-service and malware-as-a-service (Sou et al., 2013), prevent use of anonymizers and circumventors (Anonymous, 2013), investigate unknown traffic (Fan et al., 2013), actively test unknown files (Al-rimy et al., 2018), detect CnC traffic with next generation firewalls in smart grid (E-ISAC White paper, 2016), automated tracking and correlation (Liu et al., 2014), enhanced visibility into network traffic (Luo et al., 2018), restrict high risk applications and traffic (Fan et al., 2013), selective decryption and inspection of SSL traffic from IoT hosts and consumer applications (Nitti et al., 2014), drive-by-download protection (Khanna et al., 2016), block known exploits and malware (Ayar et al., 2017), limit traffic for common applications to default ports (Barreto et al., 2014).

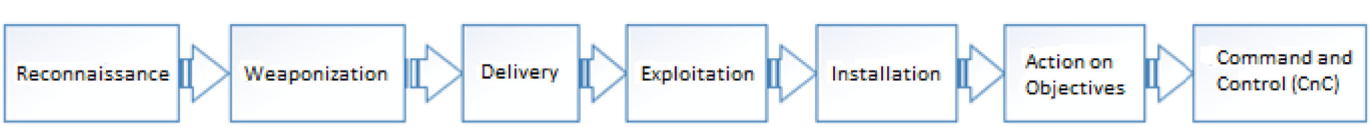


Fig. 9. Lockheed-Martin cyber kill-chain (E-ISAC White paper, 2016).

As per National Institute of Standards and Technology (NIST) directives and security policies for smart gird, AAA functions must be centrally managed and locally stored (Cherdantseva et al., 2016). Fail-back mechanisms such as hot site, warm site and cold site are set up to allow access when central control communication is down for maintenance or due to a fault. Smart grid access control credentials are user-specific rather than role-based or discretionary access (Liang et al., 2017). Biometric features such as fingerprint, iris scan and retina scan are used as credentials for user-centric access (Nitti et al., 2014). Maintenance employees typically need to access substations, IEDs, smart meters and outdoor field equipment where access is configured for both local as well as remote access based on lightweight directory access protocol (LDAP) and remote authentication dial-in user service (RADIUS) protocol (Hur, 2013).

Smart meters also act as gateways for ingress to HAN through role-based access control (RBAC), as the onus is on the customers to safeguard their access credentials (Ozay et al., 2016). Smart grid stabilization involves communication between smart meter and AMI interface where downlink demand response (DR), uplink usage, and meter-reading are achieved through mutual authentication (Wade et al., 2010). The unavailability of a user application or a user network is as impactful as CIA failure on the generation and transmission spectrum of the smart grid (Barreto et al., 2014). Though secure tunnel, key-based encryption and trust-based access are used to mitigate DoS attacks (Chen et al., 2018), argue that the NAN and HAN are susceptible to DoS attacks to a greater extent in comparison to substation networks. Lack of readily available security patches for smart grids makes them more susceptible to attacks and surreptitious data exfiltration (Xiao et al., 2013a). Interpreting and countering the cyber kill-chain decisively assists to mitigate the attack surfaces for exploitation over the smart grid cyberspace (E-ISAC White paper, 2016).

The NIST 7628 framework developed collaboratively by US government and the private sector aims to improve critical infrastructure cybersecurity, with an emphasis on risk-based cybersecurity framework (Anonymous, 2013). The standard combines industry best practices and standards to manage and reduce cybersecurity risk to critical infrastructure using next-generation advanced defense protection solutions (Anonymous, 2013). Adhering to the NIST 7628 cybersecurity framework for smart grid security calls for a collaborative and multidisciplinary approach to secure smart grid technologies amid increasing integration of energy storage, electric vehicles and renewable energy (Reka and Dragicevic, 2018). Moreover, to streamline the security implementation and management process, NIST directive outlines identifying, managing and reducing the cyber risk relying on visibility and control into critical assets and associated activities (Shafie et al., 2018). The NIST directives designed to enhance cybersecurity in critical infrastructure such as smart grids are summarized in Table 7.

5.3. Diamond model of intrusion detection in smart grids and IoT

The following characteristics facilitate undetected intrusions in minimum number of uninterruptible steps in smart grids, deviating from traditional cyber kill-chain: customized smart grid threats, IoT threats and cyber-physical system threats (Ozay et al., 2016), smart grid exploitation critically impacts the wider cyberspace such as smart cities, IoT, IIoT (Ban et al., 2016), high computational overheads to analyze Internet facing grid components in real-time (Bartoli et al., 2011), sub-microsecond accuracy requirements in smart grid communications (Wang et al., 2016a), real-time power consumption (Liang et al., 2017), eliminated or reduced manual maintenance (Karnouskos, 2012), device-control and data-collection pushed to the edge (Zou et al., 2018).

The diamond model of intrusion analysis perceives an intrusion event as a synthesis of four features described as adversary, infrastructure, capability and victim (Berger and Iniewski, 2012). The diamond intrusion detection model describes an attack as a procedural approach where a threat actor (adversary) identifies a target (victim). The adversary then

Table 7
NIST directives for securing smart grids and other critical infrastructure (Anonymous, 2013).

Category/ Subcategory of security directive	NIST directive and achievability on smart grids	Achievable Outcomes and Security Advantages
Identify	• The directive suggests mapping all ICS in smart grids, and IoT devices and an up-to-date inventory of these devices • This serves to monitor communication links and data flows between the network devices • This also facilitates real-time alerts of every cyber event that within the network. Alerts can be exported to SIEM systems for detailed analysis	• Threat detection and mitigation that combines behavioral anomalies with policy-based rules • Asset Tracking including dormant/idle devices • Vulnerability management • Configuration control to track changes to firmware, whether done through the network or locally • Enhance network visibility in the ever-morphing world of malware by categorizing smart grid devices and data as per their relative susceptibility to malicious attacks
Protect	• This directive limits access to smart grid and critical infrastructure assets and associated facilities to authorized users, processes, personnel, devices, and systems • Mandates auditing system logs, facilitating the consumption of this information by SIEM systems	• Ensures effective access permissions incorporating the principles of least privilege and separation of duties • Data-at-rest and data-in-transit protected, mitigating suspicious and unauthorized access and changes • Anomalous behavior and deviation from normal network activity can be logged over time • Facilitates legitimate remote maintenance tracking devices that are being connected or disconnected from the network
Detect	• This directive provides guidelines for tracking and tracing smart grid data items and component diagnostics, remote login commands, and consumer data (Batamuliza, 2018) • Emphasizes data correlation between multiple sources including the who, what, when, where and how for each event	• Anomalous activity detected in a timely manner • Analyze potential impact of events • A baseline of smart grid network operations • Event data aggregated and correlated from multiple sources and sensors • Ensures high availability and high security • Ensure timely and adequate awareness of anomalous events
Respond	• This directive assures timely restoration of systems and network components affected by cybersecurity events	• Coordinated response activities with stakeholders and appropriate, law enforcement agencies • Ensures consistent event reporting tracing the affected device, user, destination, protocols used and time of the event
Recover	• Ensure adequate response and recovery activities	• Provides forensic support raising an alert whenever a new vulnerability is identified

launches an attack (capability) on the target through an infrastructure (capability) possessed by the victim (Zhang et al., 2017b). The interdependence and underlying relationship among these features are represented by edge-connection resembling a diamond; hence the model is named the diamond model (Yan et al., 2012). The model views intrusion activity as a scientific principle comprising of measurement, testability and repeatability and provides a comprehensive methodology for intrusion documentation, synthesis and correlation over cyberspace (Alcaraz and Lopez, 2014). With large number of intrusion prone devices in the IoT, smart grids and cyber-physical systems landscape, the diamond intrusion model provides novel opportunities to integrate threat-intelligence in real-time for extensive and in-depth network defense (Wang et al., 2018). This threat-intelligence can enable real-time automated correlation across diverse intrusion events, classify intrusions according to severity and extent of impact, forecast adversary attempts and actions and plan intelligent mitigation strategies (Khan et al., 2017).

However, despite the best IDS technology and intrusion detection models, the human errors lead to some drawbacks such as loosely set access permissions (Melese and Avadhani, 2016), failure to change default access credentials (Melese and Avadhani, 2016), access from personally owned devices once they are inside the secure network (Melese and Avadhani, 2016), failure to activate implemented malware controls (Hui et al., 2017), failure to air gap (isolate) smart grid distribution network from internal network (Han et al., 2018), and failure to update legacy components (Melese and Avadhani, 2016). The diamond intrusion analysis model complements the smart grid cyber kill-chain by uncovering, understanding and thwarting intrusion attempts by external threat actors as well as malicious insiders (Saputro and Akkaya, 2015). The intrusion model helps investigating the questions "who, what, when, where, why, and how" about smart grid intrusion attempts while also predicting the probability of intrusion recurrence (Alcaraz and Lopez, 2014).

Analysing intrusions on smart grid and IoT devices with the aid of cyber kill-chain and diamond intrusion model has resulted in a shift from tactical mitigation (countering the threat) to strategic mitigation (countering the adversary/threat actor), and improvements in analytical efficiency and accuracy (Saputro and Akkaya, 2015). As opposed to relying on observable and tangible indictors of intrusion activity, the diamond intrusion detection model encompasses a wider mode of adversary operations to offer an informed perspective to apply CIA preservation methodologies (Zhang et al., 2017b). Specific search engines on the dark web provide reconnaissance-as-a-service and crimeware-as-a-service to attack smart grids (Kouicem et al., 2018). Adversaries utilizing these cloud-based cyber kill-chain services emulate smart grid prototypes to study underlying interweaved components to build and deliver partially and differently weaponized payloads embedded with malicious cyber capabilities (Alcaraz and Lopez, 2014). The diamond intrusion detection model is shown in Fig. 10.

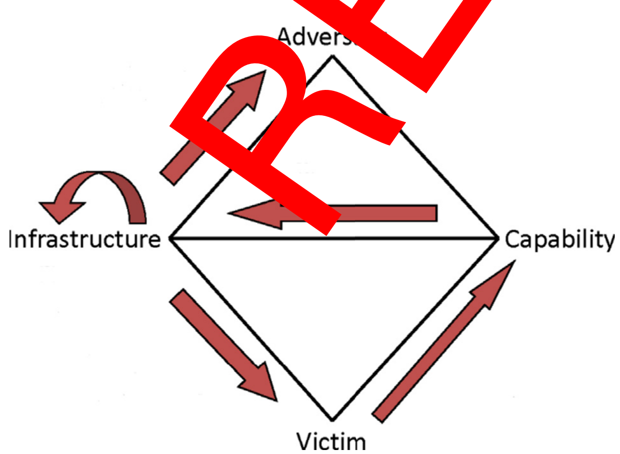


Fig. 10. Diamond intrusion detection model (Saputro and Akkaya, 2015).

5.4. Smart grids attacks: exploitation of network and architecture vulnerabilities

The IDS in smart grids is dependent on resource constraints in HAN, NAN, and FAN devices, their communication and computation overhead as well as lack of central location to install IDS (Das et al., 2018). While some researchers suggest that more intrusions can be detected by placing more IDS nodes in the network, placing a number of IDS nodes leads to more alerts and more false positives (Khan and Salah, 2018). An alternate approach is to place intelligent IDS at entry points and edge of multi-faceted and multi-purpose devices in smart grid networks (Momoh, 2012). Data correlation and statistical analysis on alerts gathered by IDS leads to increased resilience, self-healing, and recovery from a larger set of vulnerabilities in communication sensors, smart meters, gateways and peripheral devices ([illegible] et al., 2018). The IDS for HAN include consumer building devices that monitor and control electricity consumption by home devices that facilitate demand response (DR) and allow peripheral devices to react to price signals. Placing IDS in smart meters that collect user data and forward it to WAN allows electricity distribution companies to send real-time commands to end user devices (Sou et al., 2013). The WAN IDS detects intrusions on network that connects multiple substations and customers' endpoint devices (Khan and Salah, 2018). IDS in smart grids must uncover protective methodologies used throughout different cyber physical kill-chain stages (Chakhchoukh and Ishii, 2015). The physical infrastructural changes incorporated in smart grids due to migration from a centralized power generation model to distributed generation model that executes at the edge of the grid is shown in Fig. 8 (Ozay et al., 2016). The IDS provides a part of the solution but a tighter security can be achieved by using integrated threat detection and security solutions at various threat points (Liu et al., 2015). Researchers increasingly view IDS and firewalls as a single device able to self-heal, i.e. reconfigure in case of blackouts and power outages (Wade et al., 2010). Table 7 outlines some characteristics introduced with increasing two-way communication between peripheral devices and smart grids that emphasizes the need of advanced security and privacy mechanisms to safeguard the two-way communications.

Referring to Fig. 11, let us suppose an adversary targets a smart grid substation device. The attacker performs reconnaissance and tracks the location of device over GPS (Jindal et al., 2016). The attacker might decide to bypass weaponization, installation, or even command and control (CnC) phases as the successful delivery of the weaponized capability immediately exploits the substation device (E-ISAC White paper, 2016). Reconnaissance also involves determining wireless

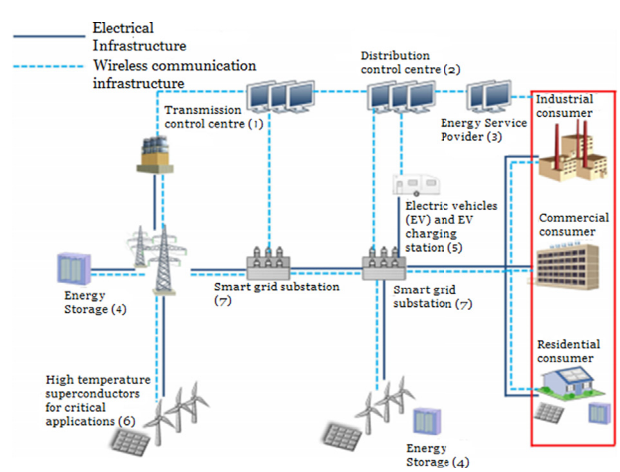


Fig. 11. Potential ingress points in smart grid two-way communication infrastructure (Ozay et al, 2016).

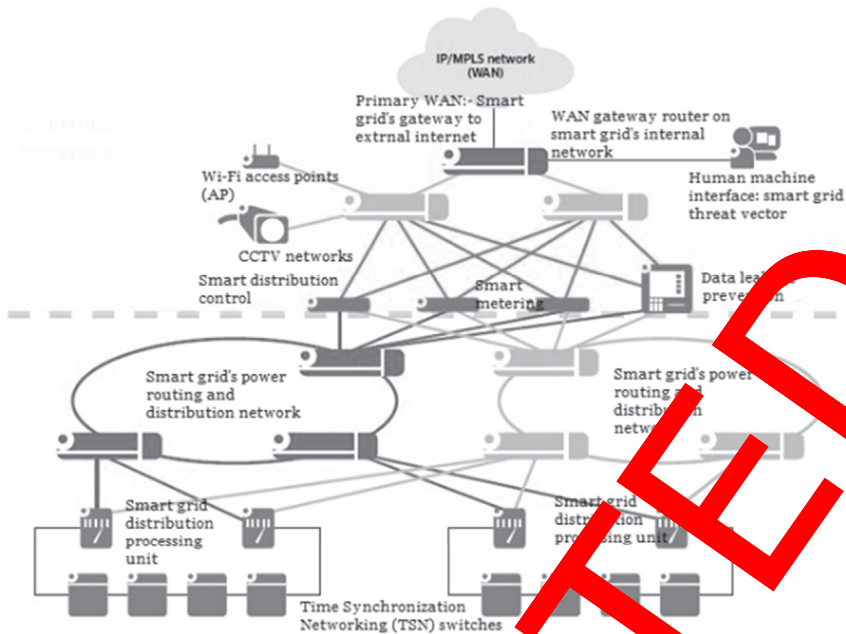


Fig. 12. Time synchronized communications and sub-microsecond accuracy requirements in smart grids open up a multitude of attack surfaces (Alcaraz et al., 2011).

frequencies and protocols used in target network and identify the service provider that facilitates the smart grid network and IoT devices' cellular connectivity. Reconnaissance phase completes with identifying target devices (Xia and Wang, 2012). Weaponization involves the procurement of a botnet to prepare programmed malware and APTs. Weaponization might also include simulating a virtual base station to provide equivalent cellular connectivity injected between the smart gird, service provider and the peripheral IoT device (Xia and Wang, 2012). Upon identifying the communication protocol and all traffic utilizing the protocol, a threat actor might commence unauthenticated communication in the smart grid network, with help of APT, gaining access to sensitive data (Kouicem et al., 2018) (see Fig. 12).

The CnC step of kill-chain enables threat actor to get access to data and architecture-centric details of smart grid that can be misused to force target homes into power outage (E-ISAC White paper, 2016). Understanding the architecture of the smart grid communication protocol with respect to users helps to execute a threat. The IDS might not immediately identify components that may be isolated, replaced, or outright removed from the smart grid network (Alcaraz and Lopez, 2014). A scheduled cyber vulnerability assessment could conclude that a smart grid peripheral device has been intruded leading to observable fluctuations in power consumption (Saxena and Grijalva, 2017). However, attacks could be conducted in a way that is nonintrusive and difficult to detect (E-ISAC White paper, 2016). Research involving electromagnetic emissions in side-channel attacks that are distinct from extraction-centric depiction revealed patterns in characterization, simulation, setup of data acquisition (Kim and Poor, 20[illegible]). Most smart grid and IoT attacks trend towards inexpensive approaches that require the minimum steps where possible due to following features of smart grids: decentralized device control (Chakhchoukh and Ishii, 2015), bringing the control systems to the desktop (Khan and Salah, 2018), continuous data acquisition (Zou et al., 2018), real-time Ethernet-based (Fan et al., 2013), wireless networks for industrial applications based on proprietary protocols (Al-rimy et al., 2018), power over Ethernet (Mendez Mena et al., 2018), converging ICT with industrial networks (Mendez Mena et al., 2018), IPv6 addressing for industrial networks (Zarpelão et al., 2017), Internet protocol for smart objects (Zarpelão et al., 2017), IoT and IIoT network convergence (Ban et al., 2016), cloud based automation services (Ban et al., 2016) (see Figs. 13 and 14).

Table 8 summarizes common network segmentation, network

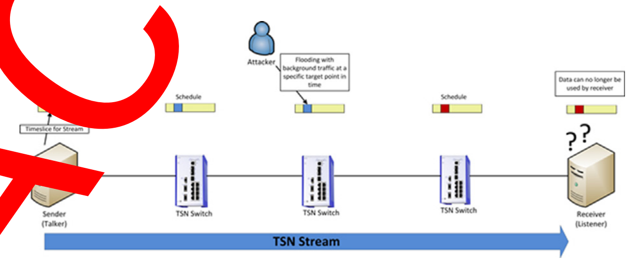


Fig. 13. Time synchronized communication between sender and receiver in smart grid (Zhao et al., 2018).

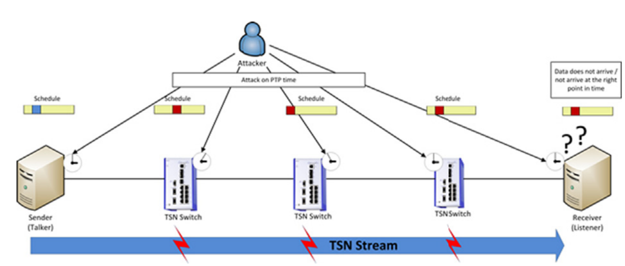


Fig. 14. Denial of service (DoS) attack on smart grid TSN stream (Zhao et al., 2018).

isolation, access control, remote access, hardware and application security mechanisms and their widespread use in conventional IT systems, SCADA, ICS and smart grid systems (Wang and Lu, 2013). The table also outlines why these mechanisms are needed to enhance effective cyber hygiene in smart grids. Access control from masqueraded IP-addresses envelops vigorous attacks against critical smart grid power distribution frameworks (Schachter and Mancarella, 2016). The interested readers may refer to (Mell et al., 2006) for a detailed description of the common vulnerability scoring system (CVSS), used to evaluate the severity of risks posed by different threats.

Wireless mesh networks to facilitate D2D communication in smart grids render the broadcast communication vulnerable to intrusion and is infeasible to be monitored by real-time intrusion sensors (Bartoli et al., 2011). A large number of studies on IDS are protocol specific and give

Table 8
Applicability, scalability and feasibility of common security mechanisms to smart grids to achieve effective cyber hygiene.

Popular network segmentation, network isolation, access control, remote access, hardware and application security mechanisms	Applicability, Scalability and Feasibility of current security mechanisms				Potential need for the security mechanism to enhance effective cyber hygiene
	IT systems	ICS	SCADA	Smart Grids	
Hardening network switch (Butun et al., 2014)	High	Medium	Medium	Low	• Total awareness of evolving threats and vulnerabilities at all times is improbable in smart grids (Butun et al., 2014) • Cybersecurity resources lack ability to identify, monitor, assess, and upgrade cyber assets and co[illegible]d smart grid network architecture (Zhu et al, 2018)
Application hardening (Butun et al., 2014)	High	Medium	Medium	Low	
DHCP servers isolation (Zhu et al., 2018)	High	Medium	Medium	Low	
DNS sever isolation (Zhu et al., 2018)	High	Medium	Medium	Low	
DHCP/DNS zone transfers (Zhu et al., 2018)	High	Medium	Medium	Low	
Firewalls, Next Generation Firewalls (NGF) (Sou et al., 2013)	High	Medium	Medium	High	• Smart grid architecture cannot rely on timely threat intelligence from Federal agencies (Sou et al., 2013)
Desk Device security (Chakhchoukh and Ishii, 2015)	High	Medium	Medium	Low	• IoT devices and peripheral cyber-physical systems adopt existing cybersecurity measures and industry-wise best practices to varying levels (Chakhchoukh and Ishii, 2015)
Mobile device security (Chakhchoukh and Ishii, 2015)	High	High	High	High	
Bring your own device (BYOD) security (Chakhchoukh and Ishii, 2015)	High	High	High	Low	
Subnetting and Network Access control (NAC) (Zhu et al., 2018)	High	High	High	High	• Generation, distribution, transmission, networks, communication, devices and third-party services offer varying levels of ease of access to threat actors (Zhu et al., 2018)
Authentication (Hashemi-Dezaki et al., 2015)	High	High	High	High	• Smart grid peripheral devices appear as easily accessible entry points to threat actors (Hui et al., 2017) • Very small aperture terminal (VSAT) devices used for remote access to smart grid have weak passwords sometimes set to default factory settings; authentication provides an added layer of cybersecurity (Liu et al., 2015)
NFC authentication (Hui et al., 2017)	High	Medium	Medium	High	
Implicit deny access control (Liu et al., 2015)	High	High	High	Low	
Whitelist access control (Liu et al, 2015)	Medium	Low	Low	High	
Encryption (Zhang et al., 2017a)	High	Medium	Medium	High	• Necessary in smart grids for privacy of smart meter communications (Zhang et al., 2017a)
Cryptography and hashing (Boussard et al., 2018)	High	Medium	Medium	Low	• Standards such as IEEEP1711 substation serial protection protocol (SSPP) are under development (Alcaraz et al., 2011)
AES, DES, PKI (Wang et al., 2006)	High	Medium	Medium	Low	
RAID and backups (Kim and Poor, 2011)	High	High	High	High	• Reduces smart grid power outages (Kim and Poor, 2011)

high detection rates in protocol specific environment such as ZigBee or BLE (Melese and Avadhani, 2016). Furthermore, cryptographic techniques such as PKI and encryption mitigate external intrusions, but do not offer sufficient defense against malicious insiders and nodes that are already authenticated into WMN (Abdrabou, 2016).

The DoS attacks such as packet dropping, false message relay etc. by malicious insiders are studied by (Liu et al., 2015). While centrally placed IDS supplement security offered by other means, such as tamper resistant seals, firewalls, encryption and authentication, such IDS are not scalable as current smart grids can have millions of smart peripheral devices (Pop et al., 2016). Distributed placement of IDS storage and computational capabilities offer ability to monitor traffic at the edge of the HAN, NAN and WAN (Han et al., 2018). Intrusion and targeted attacks at all seven layers of the open system interconnect (OSI) model are outlined in Table 9.

Physically insecure and unprotected entry points in two-way communication networks introduce intrusions leading to compromise (Khan and Salah, 2018). Intrusion at any node in a smart grid can be used to launch further attacks such as traffic modification, false data injection, and traffic monitoring attacks, replay attacks, spoofing, unauthorized authentication and access, inaccurate routing updates, and signal jamming attacks. Strategic deployment of IDS in smart grids, based on TC[illegible] be modelled for smart grids (Khanna et al., 2016; Ayar et al., 2017). Due to the large number of communicating devices in smart grids, public key infrastructure (PKI) is a suitable access control methodology to mitigate potential intrusions (Militano et al., 2017). Identity based signatures and biometric logins to identify and authenticate users and use of device-id to authenticate devices into smart grid networks can provide controlled communication on the network, and hence a wider window to lookout for malicious intrusions and unauthorized communication (Wang et al., 2006).

The authors in (Boussard et al., 2018) have studied DoS, energy fraud and targeted disconnect in AMI, however, this work does not propose reliable and efficient built-in IDS in AMI or smart metering infrastructure. The authors in (Butun et al., 2014) have surveyed key functional requirements for IDS in smart grids and suggested a hybrid IDS approach. However, their study concentrated only on the HAN part. Ref (Karnouskos, 2012). suggested a specification-based IDS that used protocol specifications, security requirements and security policies to monitor network activities. The approach was expensive as it needed additional IDS sensors to be deployed and increased computational overhead and payload of devices (Leszczyna, 2018a).

Both NAN and HAN offer vast landscape for exploitation (Komninos et al., 2014) because of inherent design weaknesses in used communication protocols, challenging the conventional Lockheed Martin cyber-kill chain with respect to smart grids (E-ISAC White paper, 2016). Whilst most of the above recommended techniques to achieve the CIA triad are not limited to the scope of intrusion detection and prevention as per the kill-chain model, yet they address intrusions with respect to DoS attacks across smart grids (McCary and Xiao, 2014). The IoT nodes are attacked using inexpensive strategies with minimal steps whenever feasible. Due to computational resource constraints in smart grids (Momoh, 2012), prefer IDS and NGFs to be implemented in layers, which prevents attackers from bypassing steps from the traditional kill-chain models. The IDS placed at vulnerable attack points improve the existing cyber kill-chain, offer better compatibility with attacker-centric,

Table 9
Smart grid attacks corresponding to OSI layers.

OSI layers	Possible smart grid attacks due to external intrusion
Physical layer	Eavesdropping, jamming, malicious payload manipulation (Ge et al., 2017)
Datalink layer	Spoofing, man in the middle (MITM) (Ge et al., 2017; Khanna et al., 2016)
Network layer	False updates in routing table, wormhole attack, blackhole and grayhole attacks, packet dropping, insider attacks (Ge et al., 2017); (Anonymous, 2013)
Transport layer	SYN flood, false data injection (Khan and Salah, 2018) (Ge et al., 2017)
Session layer	Key distribution attacks, advanced persistent threat (APT) attacks, encrypted attacks (Ge et al., 2017)
Presentation layer	Obfuscation attacks, tunneling attacks (Liu et al., 2015)
Application layer	End user device attacks, attacks on open source operating systems in HAN (Ashraf and Habaebi, 2015)

structure-centric, and asset-centric attacks, providing enhanced real-time capability to monitor large networks (Brown et al., 2012). Strategically placed IDS throughout the breadth of smart grids' technical complexity mitigate the risks posed by human error or outright negligence and prioritize network segments based on threat impact on their operation (Zhu et al., 2018). Moreover, the malicious abilities manifested due to limited control exercised by security practitioners to stop human beings from opening an attachment without caution, such as e-mails that lack virtual certificates is countered through data-centric intrusion detection techniques (Butun et al., 2014).

Table 10 discusses and summarizes the recommended security techniques in addition to IDS that are used in smart grids to mitigate cyber threats. In addition to examining the research objective and applicability of each of these techniques to the evolving IoT-enabled smart grid architecture, the table also identifies those steps of the cyber kill-chain that are mitigated by one or more of these security techniques.

5.5. Summary and insights

In this section, we surveyed the prevalent security measures used to counter cyber threats and attackers as the smart utilities get increasingly exposed to new threats. As attack vectors multiply and attack techniques get more sophisticated, threat detection and intelligence leverage emerging cybersecurity technologies in the age of big data and advanced analytics. While the traditional models of security management limit effectiveness as cyber adversaries continue to evolve and grow in sophistication, it is essential to proactively address the cyber risks faced by preparing in advance for an inevitable attack. Moreover, machine learning and AI offer enhanced network visibility for deeper analysis, identification, and better correlation with threat intelligence. Automated threat-seekers enabled by AI continuously scan a smart grid's environment for any changes that might indicate a potential threat. They learn from what they discover and then take proper actions such as:

- Maintain network performance even under attack
- Provide visibility into the amount of bot traffic accessing a network
- Reduce the impact of bots on critical infrastructure network during peak traffic hours
- Provide visibility into prior behavior of individual IP addresses
- Additional layer of defense based on recent client behavior
- Divert attackers from targeting the actual network
- Audit and report user activity for proactive protection against malware

6. Case study: denial of service attack on time synchronized smart grids

6.1. Adoption of TSN in smart grids, IoT, and IIoT

The IIoT and smart grids consist of various pieces constantly communicating with each other leading to enhanced automation flexibility and efficiency (Saputro and Akkaya, 2017). This relies on the aptness of the underlying communication infrastructure to deliver information to a destination and consequently receive messages in a reliable and pre-computable time frame. As seen from Fig. 9, smart grids consist of a myriad of interconnected intelligent devices constantly transmitting data resulting in pronounced traffic and bandwidth issues (Barreto et al., 2014). Various attack surfaces are introduced due to time synchronized and sub-microsecond accuracy requirements in smart grid real-time communication. The WAN routers, Wi-Fi access points, cameras, smart grid power routing and distribution network, and time synchronization switches offer new attack surfaces to motivated and skilled attackers (Wang and Lu, 2013). Cloud based service-access to real time smart grid components drives the diverse network traffic. Such a scenario increases the probability of missed connections, collisions between messages, and transmission delays which could lead to disastrous outcomes (Ban et al., 2016).

One of the most pressing research questions in recent wireless networks security is to examine the possibility of attaining real-time safety and privacy over Ethernet based communication for time-triggered and scheduled networks, as in smart grids, whilst also maintaining compatibility with IEEE 802 standards (Fan et al., 2013). The IEEE time sensitive networking (TSN) is viewed as the technological advancement in Ethernet aimed to bring to fruition the standardized and universally interoperable Ethernet networks with guaranteed end-to-end latencies, less latency fluctuations and negligible packet loss in real time communication (Batamuliza, 2018). Research findings in (Al-rimy et al., 2018) suggest that TSN is rapidly gaining pace as the fundamental building block of future IoT and IIoT networks. The TSN consists of a family of recently published as well as in-preparation standards specified in the IEEE 802.1 and 802.3 working groups operating since 2012 to standardize real-time functionality in Ethernet (He et al., 2017). The IEEE TSN is a layer 2 Ethernet-based protocol that eliminates adaptability concerns due to IoT, IIoT and smart grid components being based on IPv4 or IPv6 addressing (Hur, 2013). The development of TSN standards have shown that there exist no interoperable standards that enable a bridge to detect whether or not some systems in a network conform to behaviors agreed by configuration and protocol exchanges (He et al., 2017). Devices that exceed the allocated bandwidth for one stream can prevent the network from achieving the benefits of TSN for all other streams, not just the misbehaving stream (Al-rimy et al., 2018).

Currently under development and revision at the IEEE, the TSN technology is designed to provide speed, real-time communication and predictability in IoT, and is increasingly being applied to smart grid. The TSN offers a new perspective to determinism in IEEE 802.1 and 802.2 Ethernet networks with proposed models under review by IEEE (Al-rimy et al., 2018).

Different TSN models are described as follows:

- *Centralized TSN model*: In this model, the transmitting and receiving devices communicate over a dedicated, end-to-end connection, managed through a logical centralized network configuration (CNC). The CNC utilizes current network topology information to allocate time slots for new data streams and constantly reconfigures the involved participants based on topology updates (Wang et al., 2016a).
- *Decentralized TSN model*: In this model, TSN configuration is based on the local information gathered by each participating device. The end device presents its requirements to the device switch, which distributes the information to the rest of the network (Wang et al., 2016a).
- *Hybrid TSN model*: This model blends the characteristics of centralized and decentralized models. The end devices retain the provision to present the network bandwidth requirements to the first Ethernet switch, from where the requirements are forwarded to the CNC continuing the centralized manner (Wang et al., 2016a).

6.2. TSN configuration process

The sending device (talker) commences the communication with the listening device (listener) by announcing the characteristic information regarding the data streams it intends to transmit. This characteristic information consists of stream multicast media access control (MAC) address and class of service (CoS) priorities (He et al., 2017). The listener device interested in receiving the data stream registers and receives the associated data packets through the announced information payload (He et al., 2017).

A set of TSN mechanisms are activated in the process, depending on the requirements of the transmitted stream and capabilities of the associated Ethernet switches (Al-rimy et al., 2018). The following

Table 10
Feasibility of recommended security techniques to mitigate cyberattacks and intrusion attempts in smart grids.

Recommended techniques to achieve CIA triad	Feasibility and priority in smart grids	Research objectives of the stated technique	Partly mitigates following aspects of cyber kill-chain in smart grids and IoT
Alignments of security principles with business strategy, continuity and financial goals (Hur, 2013)	High, but highest priority lies with adherence to laws and regulations	• Network operation from control centers deployed across the WAN provide oversight and management of the entire grid (Zarpelão et al., 2017) • Complex but automated substations form the energy distribution framework (Hur, 2013)	Reconnaissance, Installation
Organizational processes (Zou et al., 2018)	Medium priority	• Reduced exposure to high voltages (Zarpelão et al., 2017) • Grid reliability and worker safety (Hur, 2013) • Location-aware dispatching (Zou et al., 2018)	Reconnaissance, Installation
Due diligence/due care (Koo et al., 2017)	Medium priority	• Future proof network convergence	Installation, CnC
Compliance: Regulatory, Legislative, Municipal, Provincial and Federal (Koo et al., 2017)	Utmost priority	• Increased employee safety through wearables powered smart meters (Koo et al., 2017) • Faster consumer response time (Liu et al., 2014) • Secure utility operations and facilities (Zhang et al., 2013) • Ensure compliance with regulations on both smart grid distribution substation side and utility side (Koo et al., 2017)	Reconnaissance, Installation,
Trans-border data flow and data breaches (Zhang and Sankar, 2016)	High priority	• Adherence to cyber kill-chain and diamond intrusion detection models (McCa[illegible] and Xiao, 2014)	CnC, Actions on objectives
Identifying threats, determining potential adversaries, threats and risk frameworks (Qiu et al., 2011)	High priority	• Continuously monitor network traffic to identify anomalies and neutralize cyberattacks before they execute the intended actions on the objective (Abawajy et al., 2018)	Weaponization, Exploitation, Delivery
Third-party assessment (Zhang and Sankar, 2016)	Low, as private consumer data should be protected from leakage	• Smart grid utility spectrum is estimated to have a large connection of intelligent smart IoT devices (Sou et al., 2013) • Integrity of each device (Berger and Iniewski, 2012) • Integrity of data generated at each device of the edge (Liu et al., 2014) • Increased device lifecycle (Pop et al., 2016)	Reconnaissance, Weaponization
Periodic reviews for consistency (Kim and Poor, 2011)	Medium to high priority depending on applications	• Business intelligence based on data used to measure key performance indicators (KPI) (Xiao et al., 2013a)	Reconnaissance, Weaponization
Government data classification (Li et al., 2012)	High priority	• Extend the IT infrastructure application to substations Comply with regulations such as NERC CIP, IEC and IEEE 1613 (Xia and Wang, 2012)	Reconnaissance, Weaponization
Consumer data classification (Li et al., 2012)	High priority	• Protect private information that is vulnerable to inference attacks ([illegible] et al., 2018) • Prevent revealing user activities such as types of appliances used at specific times and times when the home is occupied or is vacant (Anonymous, 2013)	Reconnaissance, Weaponization
Appropriate data retention policy (Ban et al., 2016)	High priority	• Autonomous data transmission among utility devices and smart metres (Bartoli et al., 2011) • Storage in cloud data centers (Ban et al., 2016)	Reconnaissance, Weaponization
Layered data handling requirements (Han et al., 2018)	High priority	• Edge computing and software defined networking (SDN) based security solutions and in WANs (Lin and Bergmann, 2016) • Statistical data analysis at the smart grid network edge (Kim and Poor, 2011); (Liu et al., 2014) • Remote device management (Zhang and Sankar, 2016) • Compute and move data to right places at right time (Zou et al., 2018)	Reconnaissance, Weaponization, Exploitation, Installation
Updated security controls and countermeasures (Sun et al., 2018)	High priority	• Remote monitoring of substation equipment for better visibility (Zhang and Sankar, 2016)	Delivery, Exploitation, Installation
Protection rings and network segregation (Zhu et al., 2018)	Low priority	• Network isolation and network segmentation (less preferred to defense-in- depth and built-in security) (Zhu et al., 2018)	Exploitation, CnC
Identifying vulnerabilities [illegible] architecture (Alcaraz and Lopez, 2014)	Medium to high priority depending on applications	• Advanced malware propagation (Momoh, 2012) • Virtualization attack propagation (Luo et al., 2018)	Exploitation, Installation
Implementing recovery procedures (Ban et al., 2016)	Medium to high priority depending on applications	• A mix of advanced and legacy services and protocols on a highly efficient communication network (Pop et al., 2016) • Automatic failback to cold site, warm site and hot site (Ban et al., 2016) • Manual recovery (Ban et al., 2016)	Installation, Actions on objectives
Secure communication channel design (Xia and Wang, 2012)	High priority	• Ethernet and other state-of-the-art networking technologies (Xia and Wang, 2012)	Installation, CnC
OSI TCP/IP model adherence (Xia and Wang, 2012)	High priority	• NAN connected smart meters (Bartoli et al., 2011) • Streetlight, distributed energy sources (Tsai and Lo, 2016) • Using wireless mesh, Bluetooth mesh (Xia and Wang, 2012)	CnC, Actions on objectives

(continued on next page)

Table 10 (*continued*)

Recommended techniques to achieve CIA triad	Feasibility and priority in smart grids	Research objectives of the stated technique	Partly mitigates following aspects of cyber kill-chain in smart grids and IoT
Protecting cryptographic keys, key escrow, key recovery and key management, public key infrastructure (PKI) (Xiao et al., 2013b)	Medium to high priority depending on applications, leads to high computational overhead	• Eases the burden of connecting legacy technologies and protocols (Tsai and Lo, 2016) • Symmetric and asymmetric key cryptography adds to payload and transmission overheads (Wang et al., 2006) • Massive key size depletes computational powers of peripheral devices (Boussard et al., 2018) • Protection is weak if symmetric key is shared among participating devices (Militano et al, 2017)	Exploitation, CnC
Control physical and logical access to assets (Liu et al., 2015)	High priority	• Power over Ethernet (PoE) allows dispensing with separate networks for automation and video surveillance (Batamuliza, 2018) • Allows cameras to operate solely on Ethernet (Batamuliza, 2018) • QoS to support mission critical applications in smart grid (Cardenas et al., 2014)	Exploitation, Installation, Actions on objectives
Identification and authentication of devices (Hui et al., 2017)	Utmost to High priority	• Streamlined information and data exchange in smart grid communications network (Liu et al., [illegible]4) • Means to preserve signal integrity (Boussard et al., 2018)	Delivery, Exploitation, Installation
Identification and authentication of people (Schachter and Mancarella, 2016)	Utmost to High priority	• Distribution automation based IP networks provide wireless connectivity and remote login to help maintenance workers [illegible] outages faster (Zarpelão et al., 2017) • Ensure non-repudiation (Hur, 2013)	Delivery, Exploitation, Installation, Actions on objectives
Single/multifactor authentication (Schachter and Mancarella, 2016)	Utmost to High priority	• Capable of two way communication with [illegible] utility network (Schachter and Mancarella, 2016)	Delivery, Exploitation, Installation
Accountability towards internal/insider threat (Khan et al., 2017)	Utmost to High priority	• Isolate the smart grid network from control center, substation, [illegible]AN, HAN, utilities and mobile workforce (Bartoli et al., 2011) • Monitor critical networks to identify anomalies and mitigate threats ([illegible] et al., [illegible]) • Detect tampering with field devices and device settings ([illegible] and Lo, 2016)	Delivery, Exploitation, Installation, Actions on objectives
Integrated credential management (Han et al., 2018)	Utmost to High priority	• Converge [illegible] multiple proprietary systems into a single IP framework (Hur, 2013)	Delivery, Exploitation, Installation, Actions on objectives
Continuous egress monitoring (Hui et al., 2017)	High priority	• Improved process visibility, usually achieved by NGF (Khan et al., 2016)	CnC
Integrated identity-as-a-service (Schachter and Mancarella, 2016)	High priority	• Allows customers to make informed choices about electricity consumption (Ayar et al., 2017)	Delivery, CnC
End-user energy consumption profiling (Pop et al., 2016)	High priority	• [illegible]d response (Alaba et al., 2017)	CnC
Deep packet inspection (Xiao et al., 2013a)	Utmost to High priority	• Intelligent intrusion detection to look for obfuscated malware (Ippolito et al., 2014)	Delivery, CnC
Virtual and cloud asset inspection (Ban et al., 2016)	Medium to high priority depending on applications	• Reliably scale to connect and monitor millions of smart meters (He et al., 2017) • Network equipment supports edge application deployment (Wade et al., 2010)	Exploitation, Installation, CnC, Actions on objectives
Log reviews and interface testing, principle of least privilege, principle of need-to-know (Zhang and Sankar, 2016)	Medium priority	• Terabytes of data generated and extracted from IoT devices delivered to right applications at the right time (Zhu et al., 2018) • Security mechanisms for reliability, availability and interoperability (Anonymous, 2013)	Exploitation, Installation, CnC, Actions on objectives
Identity issuance and data security (Melese and Avadhani, 2016)	[illegible] priority	• Remote logging for troubleshooting (Melese and Avadhani, 2016)	CnC, Actions on objectives
Virtual private network (VPN) based encryption (Schuurman et al., 2012)	Medium to high priority	• Remotely connect and isolate meters form load, power management (Melese and Avadhani, 2016)	Actions on objectives

mechanisms and components allow TSN to incorporate a strong level of determinism to IoT and IIoT data communication:

- *Time-aware scheduler*: The time-aware scheduler (TAS), defined under the IEEE 802.1Qbv introduces the capability of scheduling transmission of Ethernet frames based on CoS priorities and required transmission time (Wang et al., 2016a). This mechanism enables guaranteed data forwarding and delivery at a pre-defined point in time. TSN divides time into various equal-length segments known as cycles that provide dedicated time-slots for transmitting data packets based on real-time requirements (Wang et al., 2016a).
- *Best effort Ethernet traffic*: As an amendment to TAS, this mechanism provides capability to temporarily interrupt the current Ethernet traffic to forward time-sensitive high priority traffic (Wang et al., 2016a). The TAS efficiently classifies high-priority traffic from background traffic using CoS priorities encapsulated in virtual local area network (VLAN) tag of the Ethernet headers (Wang et al., 2016a).
- *Gate control list*: This mechanism determines which traffic queue should transmit at a specific point in time within the cycle (Wang et al., 2016a). This mechanism also considers the length of time for which an entry is active. This is an integral component of TAS,

configured on each port of IoT, IIoT and smart grid network devices (Al-rimy et al., 2018).

- *Implicit guard bands*: As smart grid is composed of a myriad of interconnected and communicating devices, TSN uses store-forward switching techniques to prevent larger length Ethernet frames from intruding into subsequent time slots (Wang et al., 2016a).
- *Precision time protocol*: Time and time-slot synchronization on all network devices is one of the fundamental requirements for TSN to function. The IEEE 1588 precision time protocol is the recommended standard used to distribute uniform time across a smart grid and IoT network (He et al., 2017; Wang et al., 2016a).
- *Traffic shapers*: Traffic shaper is the TSN mechanism that allows the reservation of the maximum required bandwidth for real-time time-sensitive data transmission within a specific time interval (Wang et al., 2016a). Using traffic shapers, the data stream to be conveyed across the talker and receiver is transformed into a type and form that ascertains the achievement of specified latency limits. The TSN as well as its predecessor time synchronization technology known as IEEE Audio-video bridging (AVB) describe three traffic shaping mechanisms currently undergoing standardization (He et al., 2017; Wang et al., 2016a).

6.3. Current IEEE 802.1 TSN standards

- *IEEE 802.1Qav:* This protocol defines the forwarding and queuing enhancements for time-sensitive streams and provisions maximum required bandwidth in real-time (Fan et al., 2013). This protocol is used in smart grids to provide guaranteed time-sensitive, bounded latency, loss-sensitive, real-time audio-video traffic based on per priority ingress metering, priority regeneration, and time-aware queueing (Wang et al., 2016a).
- *IEEE P802.1Qch:* This standard reduces the payload requirements for cyclic queuing and forwarding and specifies synchronized cyclic queuing to synchronize transmission to achieve zero congestion loss and deterministic latency regardless of network topology (Al-rimy et al., 2018). This improvement provides much simpler determination of network delays, reduces delivery jitter, and simplifies provision of deterministic services across bridged local area networks (LAN) (Fan et al., 2013).
- *IEEE P802.Qcr:* The standard for asynchronous traffic shaping specifies procedures for a bridge to perform asynchronous traffic shaping over full-duplex links with constant data rates (Fan et al., 2013). This standard provides an additional layer of shaped egress queues to merge flows into the existing queue structure with worst-case delay analysis in static network configurations (Al-rimy et al., 2018). Smart grids and peripheral IoT device traffic need zero congestion loss and deterministic latency for synchronous communication (Xia and Wang, 2012).
- *IEEE 802.1Qci:* This protocol defines per-stream filtering and policing to perform frame counting, filtering, policing and service class selection for frames. Policing and filtering functions include the detection and mitigation of disruptive transmissions by other systems in a network and improving the robustness of that network (Al-rimy et al., 2018).

The TSN attacks exploit constraints in guard bands, time-function, latency requirements and network costs imposed by infrastructural restriction (Alcaraz et al., 2011). While TSN is viewed as the future of IIoT and smart grid, yet it is crucial for smart grid designs to consider ingrained cybersecurity requirements, combining existing security principles with best policies for streamlined and organized security (Cardenas et al., 2014). The TSN utilizes time division multiple access (TDMA) and IEEE 1588 precision time protocol (PTP) to obtain synchronization, that opens up avenues for new attack vectors (Wang et al., 2016a). Some of the available TSN standards with specific features, and their current status are summarized in Table 11.

Table 11
Common IEEE 802.1 TSN standards applicable for use in smart grid, IOT, and IIOT networks for real-time communication requirements.

IEEE 802.1 TSN Standard	Description	Features empowering the smart grid
802.1Qbv	Time-aware shaping (per-queue based) (He et al., 2017)	Schedule traffic in queues and switched networks (Cardenas et al., 2014)
802.1Qbu	Frame pre-emption (He et al., 2017)	Real-time communicate-compute model (Pop et al., 2016), respond to external events in a timely manner (Zhao et al., 2018), reduces the size of guard bands (He et al., 2017)
802.1Asrev	Standard for local and metropolitan area networks timing and synchronization for time-sensitive applications (He et al., 2017)	Fault tolerance (Cardenas et al., 2014), multiple synchronization times (Zhao et al., 2018)
802.1CB	Redundancy (frame replication and elimination) (He et al., 2017)	Redundancy, frame replication and elimination (Pop et al., 2016)
802.1Qcc	Enhancements and improvements for stream reservation (Pop et al., 2016)	Scheduling (Zhao et al., 2018), enhances existing protocols to meet real-time reservation (He et al, 2017)
802.1Qca	Path control and reservation (Pop et al., 2016)	Find redundant paths and ensure redundancy (He et al., 2017)
802.1Qbu	Frame pre-emption (Pop et al., 2016)	Utilizes frame pre-emption to interrupt ongoing or scheduled transmission to transmit high-priority traffic (Al-rimy et al., 2018), enables low-latency communication in non-scheduled networks (Al-rimy et al., 2018)
802.1Qch	Cyclic queuing and forwarding (Pop et al., 2016)	Transmission selection algorithm to collect packets based on traffic class (Wang et al., 2016a)
802.1Qci	Per-stream filtering and policing (Pop et al., 2016)	Frame filtering on ingress ports based on arrival times, rates and bandwidth (Al-rimy et al., 2018)

6.4. Time as an attack vector

The TSN technology in smart grids introduces new cybersecurity challenges by introducing time as attack vectors (He et al., 2017). To obstruct the smart grid network functions, DoS can be attained in TSN by flooding timing and packet-priority data, overloading the network and preventing it from reaching its optimal performance capacity (Fan et al., 2013). The DoS can be attained by overloading a solitary reserved timeslot to adversely affect a particular mission-critical communication stream (Khan and Salah, 2018). An attacker, upon intruding in the network and gaining hold of critical control centers, could capture the time source, inject falsified information packets, or append synchronization data with jitter (E-ISAC White paper, 2016). These attacks sabotage the communication network as the time-sensitive end-device devices move to instant protected shutdown state upon detecting delay or jitter (Alcaraz et al., 2011). Fig. 10 depicts time synchronization communication and Fig. 11 depicts injection of DoS attack in TSN communication stream.

Although, conventional security solutions such as firewalls secure

TSN networks, however, the actual-time slots in TSN impact the implementation of some of the conventional firewall-based security measures because of following limitations:

- A perimeter network firewall investigates the payload of every incoming and outgoing packets which is infeasible in real-time (Subashini and Kavitha, 2011).
- Computational overhead of deep packet inspection (DPI) creates transmission delays beyond TSN limits (Khan et al., 2017).
- Time slot reservations may get out of synchronization with packet arrival through a firewall, leading to packet arrival at time slots for which they are no longer intended (Al-rimy et al., 2018).
- Firewalls offer real-time admission to manage access control lists and stateless packet filters, however, any slight delay is also delivered (Liu et al., 2015). Although this does not impact ordinary Ethernet networks, TSN networks, in which information transmissions depend on microsecond precision, communication gets disrupted (He et al., 2017).
- The TSN communication path and the devices at the edge of a TSN network affect transmission latency and cycle time (Al-rimy et al., 2018).
- The TSN communication paths need low and calculable transmission time offset, where slightly longer delays are tolerable at the edge devices and user spectrum of TSN community (Wang et al., 2016a). A solution for TSN is firewall technology designed to work in real-time (Butun et al., 2014).
- Defense-in-depth along with IEEE802.1X mechanisms applied to switches and routers guard the direct entry to the TSN network, introducing delay (Wang et al., 2016a).
- Media access control security (MACsec) used to authenticate, scramble, integrity-protect TSN networks introduces end-to-end transmission inactivity (Alcaraz et al., 2011).
- As TSN calls for a shared time-base on all participating devices, hijacking the master clock could inject jitters into the network sabotaging the proper alignment of time slots on smart grid devices (Tsai and Lo, 2016). Enforced time discontinuity could push the devices into safe shut down mode immediately (Wang et al., 2016a).

Table 12 summarizes various security vulnerabilities introduced in smart grids introduced due to time-synchronized communication requirements, security-policy requirements, and hardware and software requirements in smart grids' ICT infrastructure.

7. Future directions

For the smart grids to evolve and gain widespread acceptance and large-scale deployment, one of the challenges that needs to be addressed is mitigating cybersecurity threats in real-time. Based on the research findings, we propose the following future directions to enhance real-time intrusion detection and threat mitigation in 5G based smart grids and IoT networks.

- Fog-cloud collaboration in smart grids: Fog provides quick response in mission critical, time-sensitive and delay sensitive applications such as smart grids and IoT, while cloud enables other computations that are not delay sensitive (Ashraf and Habaebi, 2015). This would allow horizontal and vertical service scalability in smart grids. How to structure smart grid core network and end user services to harness advantage of horizontal and vertical capabilities of fog/cloud configuration remains an open challenge to be investigated (Ban et al., 2016).
- Authentication schemes for 5G small cell-based smart grids: Smart grids require faster and evolved multimedia broadcast and multicast communication, which is expected to be met by the 5G wireless (Liu et al., 2015). Emergency notifications can be further achieved with

Table 12
Smart grid security vulnerabilities introduced due to security policies, software/hardware/platform and communication network requirements.

Smart grid security-policy vulnerability	Software/hardware/firmware vulnerability in IoT and smart grids	Platform vulnerability in smart grids	Network vulnerability in smart grids
• Set of documents and procedures followed by organizations (Hur, 2013) • Published set of guidelines (Zou et al., 2018)	• Security as an add-on (Lin and Bergmann, 2016) • Lack of context-aware and ingrained security (Zhang et al., 2013)	• Missing patches (Butun et al., 2014) • Zero-day attacks (Butun et al., 2014)	• Delayed packet delivery (Saxena and Grijalva, 2017) • Non-convergent routing tables (Fan et al., 2015)
• Technical implementations and controls to avoid unforeseen scenarios (Han et al., 2018)	• Buffer overflow attacks (Zhu et al., 2018) • SQL injection ([illegible]aola et al., 2016) • Cross site scripting (Zhu et al., 2018) • Cross site request forgery (Zhu et al., 2018)	• Vulnerable APIs (Butun et al., 2014) • Poor anti-malware deployment (Momoh, 2012) • Virtualization vulnerability (Luo et al., 2018)	• Fallacies and error prone routing tables (Fan et al., 2015) • Incompatible IoT and D2D communication protocols (Bartoli et al., 2011) • Incompatibility with proprietary protocols (Bartoli et al., 2011)
• Technical implementations and controls to avoid unforeseen scenarios (Han et al., 2018)	• Hardware and software overloading due to bi-directional communication in smart grids (Qiu et al., 2011)	• Inadequate memory size (Ban et al., 2016) • Inadequate fault tolerance and backup (Ban et al., 2016)	• Corrupted headers/flags/ payloads (Kim and Tong, 2013)
• Technical implementations and controls to avoid undesirable outcomes (Han et al., 2018)	• Secure primary and secondary distribution substations, transmission substations, micro grids, control centers and ICT systems (Boussard et al., 2018)	• Insufficient alerts/SIEM log management (Melese and Avadhani, 2016)	• Quality of service requirements, router and switch malfunction (Hur, 2013)
• Mitigate deficiencies and reduce risk (Schachter and Mancarella, 2016)	• Privacy by design and defence-in-depth strategies (Zhu et al., 2018) • Home area network (HAN) infrastructure at consumer premises must be fool proof (Komninos et al., 2014)	• IoT and miniaturized device operating system vulnerability, lack of readily available patches (Anonymous, 2013)	• Errors due to SDN and corresponding protocols (Pop et al., 2016)

Journal of Network and Computer Applications 132 (2019) 118–148

zero delay between small cells and smart grid consumers through 5G small cells leading to optimal demand response in smart grids (Tsai and Lo, 2016). However, network attacks can affect communication as well as energy consumption. Intelligent and robust authentication schemes are seen as a solution to protect smart grid communications but the reliability of these schemes to detect and prevent common attacks is still an active area of research (Hui et al., 2017). The application of one factor, two-factor, three-factor and multifactor authentication to smart grids, without adding to communication overhead is a challenging research area (Melese and Avadhani, 2016). Moreover, we aim to investigate multifactor authentication to smart grids based on what you know (e.g., passwords), what you have (e.g., smart cards), and who are you (e.g., biometrics) as a future research direction (Liu et al., 2015).

- Privacy preservation for smart grids in 5G scenarios: As core smart grid networks and components such as FAN, HAN and NAN can be accessed by consumers through mobile devices and applications, the mechanisms to preserve privacy and secrecy of user data is an active research area (Komninos et al., 2014). Various solutions such as encryption, PKI, and key-management exist but their scalability to smart grid infrastructure and consumer base, without adding to computational overhead is a field open to research (Xiao et al., 2013b). Multiple security and privacy objectives central to smart grids are summarized in Table 9.
- Dataset for smart grid intrusion detection in 5G scenarios: Most of the IDS data collection and research has revolved around the Defense Advanced Research Projects Agency (DARPA) 1999, or the Knowledge Discovery in Databases, (KDD) 1999 data sets for almost a decade (Brown et al., 2012). The lack of relevance and validity of these datasets in mobile and 5G scenarios has prompted demands for other datasets. However, there is a lack of a dedicated dataset that pertains solely to smart grid and IoT infrastructure. The threat models disruptive to smart grids need to be simulated in these data sets and we believe that further research is needed to develop a new data set to build smart grid network intrusions (Bartoli et al., 2011).
- Application of data mining and machine learning for intrusion detection in self-healing smart grids: Machine learning and data analytics on smart grid datasets can help draw correlation among attacks and a reference pattern for detecting malicious activities (Liu et al., 2014). Designing an updated dataset is a research objective that would help identify unauthorized access attempts to smart grid ICT systems (Kim and Tong, 2013). Application of machine learning techniques to detect obfuscated malware, tunnelled threats and APTs in smart grids presents a challenging avenue for research.
- Security of time-sensitive communication in smart grids: Although TSN is viewed an indispensable to achieving real-time delay-sensitive goals in smart grids, secure TSN communication is still a possible research direction (Zhang et al., 2013). We propose researching the application of fog-cloud integration as replacement to TSN protocols so that the focus could shift on scaling existing security principles to fog, cloud and IoT (Ba[illegible] et al., 2016).
- Futureproofing through tamper proof security in IoT-enabled smart grids: We propose exploring the feasibility of futuristic and next-generation tamper proof security using Blockchain technology for authentication, authorization, and accounting (AAA) in smart grids (Khan and Salah, 2018). Theoretically, Blockchain bypasses the need for a central administrator to approve transactions between communicating devices (Malomo et al., 2018). Furthermore, with the onset of quantum computing, existing security measures are expected to become strained and the efficacy of Blockchain as a comprehensive and viable tamper-resistant security solution in smart grids presents a potential research area (Khan and Salah, 2018; Malomo et al., 2018).

8. Conclusion

In this paper, we surveyed advances in cyber threats that aim to exploit the vulnerabilities in IoT architecture in general and smart grids in particular. We introduced inherent IoT architecture and related protocols that make it vulnerable to threats. We then introduced smart grids and their role in powering smart cities, smart vehicles, and their interdependence on IoT. We discovered the advantages offered by smart grids and the privacy concerns and attack motives that make them an attractive target to threat actors. We then analyzed various motives that prompt attackers to target smart grids and how centralized or distributed placement of IDS can help to detect attacker presence or mitigate their entry into the smart grid networks.

Through an extensive research and analysis that was conducted, we were able to classify the threat actors primarily into four classes. The more advanced threat actors have sufficient technical expertise to design malware embedded in advanced persistent threats that are hideous and can bypass conventional security mechanisms. In addition, we were able to compare and classify the counter measures such as PKI, cryptography, access control, and encryption to mitigate threats in conventional computing systems, ICS/SCADA systems and smart grids. The survey investigates some crucial differences between traditional and smart grid networks that give rise to new challenges to deploy IDS in these resource constrained IoT networks. It is concluded that the devices in the smart grids and IoT ecosystem are increasingly vulnerable to advanced persistent threats as smart grids and IoT devices provide attack surfaces to threat actors exposing information assets at each layer of infrastructure to critical risk. Restricting access from the Internet to IoT device systems, and establishing usage and access policies to IoT devices can help obscure the open window for coordinated and sophisticated mass attacks that cause serious damage to smart grids.

The study also presented the systematic approach known as cyber kill-chain used by attackers to break into a critical system. The intrusions modelled using diamond intrusion detection model help security administrators and cyber defenders to tackle cyber kill-chain in a systematic manner. Lastly, we introduce the adoption of TSN to smart grids and IoT to enable real-time communication that also makes novel attack vectors accessible to attackers. Based on the vision for the next generation of smart grid connectivity, we proposed six open directions for future research.

Acknowledgements

Authors would like to acknowledge the financial support from Natural Sciences and Engineering Research Council of Canada.

References

Abawajy, J., et al., 2018. Identifying cyber threats to mobile-IoT applications in edge computing paradigm. Future Gener. Comput. Syst. 89, 525–538.
Abdrabou, 2016. A wireless communication architecture for smart grid distribution networks. IEEE Syst. J. 10 (1), 251–261.
Abreu, et al., 2018. A smart meter and smart house integrated to an IdM and key-based scheme for providing integral security for a smart grid ICT. Mobile Network. Appl. 23 (4), 967–981.
Al-rimy, A.S., Maarof, M.A., Shaid, S.Z.M., 2018. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput. Secur. 74, 144–166.
Alaba, A., et al., 2017. Internet of Things security: a survey. J. Netw. Comput. Appl. 88, 10–28.
Alavi, H., et al., 2018. Internet of Things-enabled smart cities: state-of-the-art and future trends. Measurement 129, 589–606.
Alcaraz, C., Lopez, J., 2014. WASAM: a dynamic wide-area situational awareness model for critical domains in Smart Grids. Future Gener. Comput. Syst. 30, 146–154.
Alcaraz, C., Lopez, J., Zhou, J., Roman, R., 2011. Secure SCADA framework for the protection of energy control systems. Concurrency Comput. Pract. Ex. 23 (12), 1431–1442.
Anonymous, 2013. Request for Comments on Draft NIST Interagency Report (NISTIR) 7628 Rev. 1, Guidelines for Smart Grid Cyber Security. Federal Information & News Dispatch, Inc, Washington.
Ashraf, Q.M., Habaebi, M.H., 2015. Autonomic schemes for threat mitigation in Internet of Things. J. Netw. Comput. Appl. 49, 112–127.
Auty, M., 2015. Anatomy of an advanced persistent threat. Netw. Secur. 2015 (4), 13–16.
Ayar, et al., 2017. A distributed control approach for enhancing smart grid transient stability and resilience. IEEE Trans. Smart Grid 8 (6), 3035–3044.

Ban, H.J., Choi, J., Kang, N., 2016. Fine-grained support of security services for resource constrained internet of things. Int. J. Distributed Sens. Netw. 12 (5), 7824686.

Barreto, et al., 2014. Control systems for the power grid and their resiliency to attacks. IEEE Secur. Priv. 12 (6), 15–23.

Bartoli, et al., 2011. Secure lossless aggregation over fading and shadowing channels for smart grid M2M networks. IEEE Trans. Smart Grid 2 (4), 844–864.

Batamuliza, J., 2018. Certificateless secure anonymous key distribution scheme for smart grid. Int. J. Comput. Appl. 180 (24), 7–13.

Bekara, 2014. Security issues and challenges for the IoT-based smart grid. Procedia Computer Science 34, 532–537.

Benmalek, et al., 2018. VerSAMI: versatile and scalable key management for smart grid AMI systems. Comput. Network. 132, 161–179.

Berger, L.T., Iniewski, K., 2012. Smart Grid: Applications, Communications, and Security. Wiley.

Bou-Harb, et al., 2013. Communication security for smart grid distribution networks. IEEE Commun. Mag. 51 (1), 42–49.

Boussard, M., et al., 2018. Future spaces: reinventing the home network for better security and automation in the IoT era. Sensors 18 (9), 2986.

Brown, E., et al., 2012. Improving reliability of islanded distribution systems with distributed renewable energy resources. IEEE Trans. Smart Grid 3 (4), 2028–2038.

Butun, Morgera, S.D., Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. Commun. Surv. Tutorials, IEEE 16 (1), 266–282.

Cardenas, A., et al., 2014. A framework for evaluating intrusion detection architectures in advanced metering infrastructures. IEEE Trans. Smart Grid 5 (2), 906–915.

Cavalieri, S., Regalbuto, A., 2016. Integration of IEC 61850 SCL and OPC UA to improve interoperability in Smart Grid environment. Comput. Stand. Interfac. 47, 77–99.

Chakhchoukh, Y., Ishii, H., 2015. Coordinated cyber-attacks on the measurement function in hybrid state estimation. IEEE Trans. Power Syst. 30 (5), 2487–2497.

Chen, Y., Hong, J., Liu, C., 2018. Modeling of intrusion and defense for assessment of cyber security at power substations. IEEE Trans. Smart Grid 9 (4), 2541–2552.

Chen, J., et al., 2018. Special issue on advanced persistent threat. Future Gener. Comput. Syst. 79, 243–246.

Cherdantseva, Y., et al., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27.

Chin, W., Li, W., Chen, H., 2017. Energy big data security threats in IoT-based smart grid communications. IEEE Commun. Mag. 55 (10), 70–75.

Ciavarella, S., Joo, J., Silvestri, S., 2016. Managing contingencies in smart grids via the internet of things. IEEE Trans. Smart Grid 7 (4), 2134–2141.

Colak, et al., 2016. A survey on the critical issues in smart grid technologies. Renew. Sustain. Energy Rev. 54, 396–405.

Collier, S.E., 2017. The emerging enernet: convergence of the smart grid with the in[illegible] of things. IEEE Ind. Appl. Mag. 23 (2), 12–16.

Dacier, M.C., et al., 2014. Network attack detection and defense: securing industrial control systems for critical infrastructures. Informatik-Spektrum 37 (6), 605–607.

Dalipi, F., Yayilgan, S.Y., 2016. Security and privacy considerations for IoT application on smart grids: survey and research challenges. In: IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 6[illegible]

Das, K., et al., 2018. Overview of energy storage systems in distribu[illegible] netwo[illegible]: placement, sizing, operation, and power quality. Renew. Susta[illegible] Energy R[illegible] 1205–1230.

Deng, et al., 2017. False data injection on state estimation in powe[illegible] attacks, impacts, and defense: a survey. IEEE Trans. Ind. Electro[illegible] nf. 13 ([illegible]–423.

E-ISAC White paper. On Analysis of the Cyber Attack on t[illegible] Ukrainian Pow[illegible] rid Available: https://www.nerc.com/pa/CI/ESISAC/Do[illegible]ents/E-ISAC_SANS_[illegible]ine_DUC_18Mar2016.pdf [Accessed: 01-04-2018].

Esnaola, et al., 2016. Maximum distortion attacks in [illegible]ectric[illegible]ids. IEEE Trans. Smart Grid 7 (4), 2007–2015.

Fadlullah, Z.M., Pathan, A.K., Singh, K., 2018. Smart grid internet o[illegible]s. Mobile Network. Appl. 23 (4), 879–880.

Fan, Z., et al., 2013. Smart grid communicati[illegible]s: overview of research challenges, solutions, and standardization activitie[illegible] Commun. [illegible]rv. Tutorials, IEEE 15 (1), 21–38.

Fan, Y., et al., 2015. A cross-layer defe[illegible] echanis[illegible] against GPS spoofing attacks on PMUs in smart grids. IEEE Trans. Smar[illegible]), 2659–2[illegible].

Ge, M., et al., 2017. A framework for automati[illegible]urity ana[illegible]s of the internet of things. J. Netw. Comput. Ap[illegible]2–27.

Guo, Y., et al., 2016. Preventiv[illegible]ainte[illegible]ce for advan[illegible]etering infrastructure against malware propaga[illegible]n. IEEE T[illegible] Smart Grid [illegible] (3), 1314–1328.

Han, W., Xiao, Y., 2016. P[illegible]cy preserv[illegible] G networks in smart grid: a survey. Comput. Commun. 91–[illegible]7–28.

Han, Y., et al., 2018. Modeling [illegible]g failures and mitigation strategies in PMU based cyber-physical power systems. J[illegible]l of Modern Power Systems and Clean Energy 6 (5), 944–957.

Hansen, J. Staggs, Shenoi, S., 2017. Security [illegible]alysis of an advanced metering infrastructure. International Journal of Critical Infrastructure Protection 18, 3–19.

Hao, J., et al., 2015. Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Trans. Ind. Electron. Inf. 11 (5), 1–12.

Hashemi-Dezaki, et al., 2015. Risk management of smart grids based on managed charging of PHEVs and vehicle-to-grid strategy using Monte Carlo simulation. Energy Convers. Manag. 100, 262–276.

He, et al., 2017. Impact analysis of flow shaping in ethernet-AVB/TSN and AFDX from network calculus and simulation perspective. Sensors 17 (5), 1181.

He, D., et al., 2018. Certificate less provable data possession scheme for cloud-based smart grid data management systems. IEEE Trans. Ind. Electron. Inf. 14 (3), 1232–1241.

Hossain, E., Han, Z., Poor, H.V., 2012. Smart Grid Communications and Networking. Cambridge University Press.

Hua, L., Junguo, Z., Fantao, L., 2014. Internet of things technology and its applications in smart grid. TELKOMNIKA Indones. J. Electr. Eng. 12 (2).

Huang, Z., Yuan, F., 2015. Implementation of 6LoWPAN and its application in smart lighting. J. Comput. Commun. 3, 80–85.

Hui, T.K.L., Sherratt, R.S., Sánchez, D.D., 2017. Major requirements for building smart homes in smart cities based on internet of things technologies. Future Gener. Comput. Syst. 76, 358–369.

Hur, J., 2013. Attribute-based secure data s[illegible]idden policies in smart grid. IEEE Trans. Parallel Distr. Syst. 24 (11), 2[illegible]1.

Ippolito, M.G., et al., 2014. Multi-obje[illegible]e optimized ma[illegible]ment of electrical energy storage systems in an islanded n[illegible]work with renewable [illegible]ergy sources under different design scenarios. Energ[illegible] 648–662.

Jindal, et al., 2016. Decision tree and SV[illegible]sed data anal[illegible]s for theft detection in smart grid. IEEE Trans. In[illegible]Electron. In[illegible]3), 100[illegible]016.

Jokar, Paria, Arianpoo, Nasi[illegible] Leung, Victor CM[illegible]12[illegible] survey on security issues in smart grids. Secur. Co[illegible]un. Netw[illegible]k. 9 (3), 26[illegible]3.

Kang, W.M., Moon, S.Y., [illegible]rk, J.H., 2[illegible]. An enhanced security framework for home appliances in smar[illegible]e. Huma[illegible]entric Computing and Information Sciences 7 (1), 1–12.

Karnouskos, S., 20[illegible] Asset m[illegible]ing in the [illegible]vice-oriented Internet of Things empowered [illegible]artgrid. Service[illegible]ted [illegible]mputing and Applications 6 (3), 207–214.

Khan, M.A., Sa[illegible] K., 2018. IoT secu[illegible]iew, blockchain solutions, and open challeng[illegible]e Gener. Comput. Sy[illegible]. 82, 395–411.

Khan, S., P[illegible]inson, [illegible]in, Y., 2017. Fog computing security: a review of current appli[illegible]ions and sec[illegible] solutions. J. Cloud Comput. 6 (1), 1–22.

Khanna, K., Panigrahi, B.K., [illegible]A., 2016. Data integrity attack in smart grid: optimised a[illegible] gain momentary e[illegible]omic profit. IET Gener., Transm. Distrib. 10 (16), [illegible]032–4039.

[illegible]toun, Zeadally, S., 2017. Cybersecurity and privacy solutions in smart cities. IEEE Commun. Mag. 5[illegible]3), 51–59.

[illegible], T.T., Poor, H.V., [illegible]11. Strategic protection against data injection attacks on power [illegible]rids. IEEE Trans. [illegible]art Grid 2 (2), 326–333.

Ki[illegible]g, L., 2013. [illegible] topology attack of a smart grid: undetectable Attacks and co[illegible] IEEE J. Sel. Area. Commun. 31 (7), 1294–1305.

Komninos, N., [illegible]ppou, E., Pitsillides, A., 2014. Survey in smart grid and smart home security: issues, challenges and countermeasures. Commun. Surv. Tutorials, IEEE 16 [illegible]–1954.

Ko[illegible]D., [illegible] Y., Hur, J., 2017. Privacy-preserving aggregation and authentication of multi-source smart meters in a smart grid system. Appl. Sci. 7 (10), 1007.

[illegible]ouicem, E., Bouabdallah, A., Lakhlef, H., 2018. Internet of things security: a top-down survey. Comput. Network. 141, 199–221.

[illegible]oundinya, K., Sharvani, G., Rao, K.U., 2016. Calibrated security measures for centralized IoT applications of smart grids. In: International Conference on Computation System and Information Technology for Sustainable Solutions, pp. 153–157.

Le, N., Chin, W., Chen, H., 2017. Standardization and security for smart grid communications based on cognitive radio technologies-A comprehensive survey. Commun. Surv. Tutorials, IEEE 19 (1), 423–445.

Lee, S., Kim, J., Shon, T., 2016. User privacy-enhanced security architecture for home area network of Smart grid. Multimed. Tool. Appl. 75 (20), 12749–12764.

Lemay, et al., 2018. Survey of publicly available reports on advanced persistent threat actors. Comput. Secur. 72, 26–59.

Leszczyna, R., 2018. A review of standards with cybersecurity requirements for smart grid. Comput. Secur. 77, 262–276.

Leszczyna, R., 2018. Cybersecurity and privacy in standards for smart grids – a comprehensive survey. Comput. Stand. Interfac. 56, 62–73.

Liang, W., et al., 2017. A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid 8 (4), 1630–1638.

Li, H., et al., 2012. Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Trans. Smart Grid 3 (3), 1540–1551.

Lim, H., Taeihagh, A., 2018. Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. Energies 11 (5), 1062.

Lin, H., Bergmann, N.W., 2016. IoT privacy and security challenges for smart home environments. Information 7 (3), 44.

Liu, X., Li, Z., 2017. False data attack models, impact analyses and defense strategies in the electricity grid. Electr. J. 30 (4), 35–42.

Liu, J., Xiao, Y., Gao, J., 2014. Achieving accountability in smart grid. IEEE Syst. J. 8 (2), 493–508.

Liu, R., et al., 2015. Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Trans. Smart Grid 6 (5), 2444–2453.

Luo, X., et al., 2018. Observer-based cyber-attack detection and isolation in smart grids. Int. J. Electr. Power Energy Syst. 101, 127–138.

Ma, S., Zhang, H., Xing, X., 2018. Scalability for smart infrastructure system in smart grid: a survey. Wireless Pers. Commun. 99 (1), 161–184.

Malomo, O.O., Rawat, D.B., Garuba, M., 2018. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. J. Supercomput. 74 (10), 5099–5126.

McCary, Xiao, Y., 2014. Malicious device inspection in the HAN smart grid. In: Proceedings of the International Conference on Security and Management (SAM), p. 1.

RETRACTED

Melese, S.Z., Avadhani, P.S., Andhra University CS&SE, Visakhapatnam, 530003, India, 2016. Honeypot system for attacks on SSH protocol. Int. J. Comput. Netw. Inf. Secur. 8 (9), 19–26.

Mell, P., Scarfone, K., Romanosky, S., 2006. Common vulnerability scoring system. IEEE Secur. Priv. 4 (6), 85–89.

Mendez Mena, D., Papapanagiotou, I., Yang, B., 2018. Internet of things: survey on security. Inf. Secur. J. A Glob. Perspect. 27 (3), 162–182.

Militano, L., et al., 2017. NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5G systems. Future Internet 9 (3), 31.

Minoli, D., Sohraby, K., Occhiogrosso, B., 2017. IoT considerations, requirements, and architectures for smart buildings-energy optimization and next-generation building management systems. IEEE Internet of Things Journal 4 (1), 269–283.

Momoh, A., 2012. Smart Grid: Fundamentals of Design and Analysis.

Nardelli, P.H.J., Kuhnlenz, F., 2018. Why smart appliances may result in a stupid grid: examining the layers of the sociotechnical systems. IEEE Systems, Man, and Cybernetics Magazine 4 (4), 21–27.

Nitti, M., Girau, R., Atzori, L., 2014. Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. 26 (5), 1253–1266.

Ozay, M., et al., 2016. Machine learning methods for attack detection in the smart grid. IEEE Transactions on Neural Networks and Learning Systems 27 (8), 1773–1786.

Pop, et al., 2016. Design optimisation of cyber-physical distributed systems using IEEE time-sensitive networks. IET Cyber-Physical Systems: Theory & Applications 1 (1), 86–94.

Qiu, R.C., et al., 2011. Cognitive radio network for the smart grid: experimental system Architecture, control algorithms, security, and microgrid testbed. IEEE Trans. Smart Grid 2 (4), 724–740.

Reka, S.S., Dragicevic, T., 2018. Future effectual role of energy delivery: a comprehensive review of Internet of Things and smart grid. Renew. Sustain. Energy Rev. 91, 90–108.

Saputro, Akkaya, K., 2015. PARP-S: a secure piggybacking-based ARP for IEEE 802.11s-based Smart Grid AMI networks. Comput. Commun. 58, 16–28.

Saputro, N., Akkaya, K., Uludag, S., 2012. A survey of routing protocols for smart grid communications. Comput. Network. 56 (11), 2742–2771.

Saxena, N., Grijalva, S., 2017. Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication. IEEE Trans. Ind. Electron. Inf. 13 (3), 1482–1491.

Schachter, A., Mancarella, P., 2016. A critical review of Real Options thinking for valuing investment flexibility in Smart Grids and low carbon energy systems. Renew. Sustain. Energy Rev. 56, 261–271.

Schuurman, et al., 2012. Smart ideas for smart cities: investigating crowdsourcing for generating and selecting ideas for ICT innovation in a city context. Journal of Theoretical and Applied Electronic Commerce Research 7 (3), 12–49.

Sha, K., et al., 2018. On security challenges and open issues in Internet of Things. Future Gener. Comput. Syst. 83, 326–337.

Shafie, E., et al., 2018. Impact of passive and active security attacks on MIMO smart grid communications. IEEE Syst. J. 1–4.

Sharma, K., Saini, L.M., 2017. Power-line communications for smart grid: progress, challenges, opportunities and status. Renew. Sustain. Energy Rev. [illegible]51.

Shaukat, N., et al., 2018. A survey on electric vehicle transportation within smart grid system. Renew. Sustain. Energy Rev. 81, 1329–1349.

Singh, S., Jeong, Y., Park, J.H., 2016. A survey on cloud computing security: issues, threats, and solutions. J. Netw. Comput. Appl. 75, 200–222.

Sood, K., Enbody, R.J., 2013. Targeted cyberattacks: a superset of advanced persistent threats. IEEE Secur. Priv. 11 (1), 54–61.

Sou, K.C., et al., 2013. On the exact solution to a smart grid cyber-security analysis problem. IEEE Trans. Smart Grid 4 (2), 856–865.

Srivastava, K., et al., 2018. Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information. Journal of Modern Power Systems and Clean Energy 6 (5), 887–899.

Subashini, S., Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34 (1), 1–11.

Sun, C., Hahn, A., Liu, C., 2018. Cyber security of a power grid: state-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56.

Talari, S., et al., 2017. A review of smart cities based on the internet of things concept. Energies 10 (4), 421.

Tan, et al., 2017. Survey of security advances in smart grid: a data driven approach. Commun. Surv. Tutorials, IEEE [illegible]), 397–422.

Tsai, J., Lo, N., 2016. Secure anonymous key distribution scheme for smart grid. IEEE Trans. Smart Grid 7 (2), [illegible]–914.

Wade, N.S., et al., 2010. Evaluating the benefits of an electrical energy storage system in a future smart grid. Energy Policy 3[illegible] (11), 7180–[illegible]8.

Wadhawan, Y., AlMajali, A., Neuman, C., 2018. A comprehensive analysis of smart grid systems against cyber-physical attacks. Electronics 7 (10), 249.

Wan, Z., et al., 2014. SKM: scalable key management for advanced metering infrastructure in smart grids. IEEE Trans. Ind. Electron. 61 (12), 7055–7066.

Wang, W., Lu, Z., 2013. Cyber security in the smart grid: survey and challenges. Comput. Network. 57 (5), 1344–1371.

Wang, L., Liu, A., Jajodia, S., 2006. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. Comput. Commun. 29 (15), 2917–2933.

Wang, Q., et al., 2016. Coordinated scheme of under-frequency load shedding with intelligent appliances in a cyber physical power system. Energies 9 (8), 630.

Wang, X., et al., 2016. Detection of command and control in advanced persistent threat based on independent access. In: IEEE International Conference on Communications (ICC), pp. 1–6.

Wang, et al., 2018. Deep learning based interval state estimation of AC smart grids against sparse cyber attacks. IEEE Trans. Ind. Electron. Inf. 14 (11), 4766–4778.

Xia, J., Wang, Y., 2012. Secure key distribution for the smart grid. IEEE Trans. Smart Grid 3 (3), 1437–1443.

Xiang, Y., Wang, L., Liu, N., 2017. Coordinated attacks on electric power systems in a cyber-physical environment. Electr. Power Syst. Res. 149, 156–168.

Xiao, Z., Xiao, Y., Du, D.H., 2013. Exploring malicious meter inspection in neighborhood area smart grids. IEEE Trans. Smart Grid 4 (1), 214–226.

Xiao, Z., Xiao, Y., Du, D.H.-, 2013. Non-repudiation in neighborhood area networks for smart grid. IEEE Commun. Mag. 51 (1), 18–26.

Xin, Y., et al., 2018. Machine learning and deep learning methods for cybersecurity. IEEE Access 6, 35365–35381.

Yan, et al., 2012. A survey on cyber security for smart grid communications. Commun. Surv. Tutorials, IEEE 14 (4), 998–10[illegible].

Yoo, Shon, T., 2016. Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: vulnerabilities, security requirements, and security architecture. Future Gener. Comput. Syst. 61, 128–136.

Zarpelão, B., et al., 2017. A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. 84, 25–37.

Zaveri, M.A., Pandey, S.K., K[illegible]ar, J.S., 2016. Co[illegible]e service oriented smart grid using the internet of things. In: International Conference on Communication and Signal Processing, pp. 1716–1722.

Zhang, J., Sankar, L., 2[illegible]. Physical system consequences of unobservable state-and-topology cyber-physical attacks. IEEE Trans. Smart Grid 7 (4), 2016–2025.

Zhang, Y., Chen, W., Gao, W., 2[illegible]. A survey on the development status and challenges of smart grids in main driver countries. Renew. Sustain. Energy Rev. 79, 137–147.

Zhang, Y., Xiang, Y., Wang, L., 2017. [illegible] system reliability assessment incorporating cyber attacks against wind farm energy management systems. IEEE Trans. Smart Grid 8 (5), [illegible]3–233[illegible].

Zhang, Z., et al., 2013. [illegible] synchronization attack in smart grid: impact and analysis. IEEE Trans. Smart Grid [illegible], 87–98.

Zhao, [illegible], [illegible]p, P., Craciunas, S.S., 2018. Worst-case latency analysis for IEEE 802.1Qbv time sensitive networks using network calculus. IEEE Access 6, 41803–41815.

[illegible], Y., et al., 2015. Joint substation-transmission line vulnerability assessment against the smart grid. IEEE Trans. Inf. Forensics Secur. 10 (5), 1010–1024.

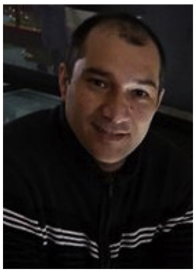
[illegible], et al., 2018. Big data mining of users' energy consumption patterns in the wireless smart grid. IEEE Wireless Communications 25 (1), 84–89.

Zik[illegible], [illegible]B., et al., 20[illegible]. A survey on routing protocols supported by the Contiki Internet of [illegible]g system. Future Gener. Comput. Syst. 82, 200–219.

Zou, X., et al., 2018. A novel network security algorithm based on improved support vector machine from smart city perspective. Comput. Electr. Eng. 65, 67–78.

Abhishek Gupta received his BE (Electronics and Telecommunication) from Pune University, India and MSc (Computational Intelligence) from De Montfort University, Leicester, United Kingdom, respectively. He is currently a MASc candidate at WINCORE Labs in the Dept. of Electrical and Computer Engineering, Ryerson University, Toronto, Canada under the supervision of Prof. Alagan Anpalagan. His research and scientific interests are related to machine learning, self-driving cars, wireless communication, cloud computing, and cyber security. He holds CompTIA A+, Network+ and Cloud + certifications. His current research work is pivoted on application of machine learning techniques to enhance secure communication in autonomous vehicles.

Alagan Anplagan received the B.A.Sc. M.A.Sc. and Ph.D. degrees in Electrical Engineering from the University of Toronto, Canada. He joined the Department of Electrical and Computer Engineering at Ryerson University in 2001 and was promoted to Full Professor in 2010. Dr. Anpalagan directs a research group working on radio resource management (RRM) and radio access & networking (RAN) areas within the WINCORE Lab. His current research interests include cognitive radio resource allocation and management, wireless cross layer design and optimization, cooperative communication, M2M communication, small cell networks, and green communications technologies. Dr. Anpalagan serves as Associate Editor for the IEEE Communications Surveys & Tutorials (2012-), IEEE Communications Letters (2010–13) and Springer Wireless Personal Communications (2009-), and past Editor for EURASIP Journal of Wireless Communications and Networking (2004–2009). He co-authored of three edited books, Design and Deployment of Small Cell Networks, Cambridge University Press (2014), Routing in Opportunistic Networks, Springer (2013), Handbook on Green Information and Communication Systems, Academic Press (2012). He is a registered Professional Engineer in the province of Ontario, Canada.



Glaucio H.S. Carvalho is a Professor of the School of Applied Computing, Faculty of Applied Science and Technology (FAST) at Sheridan College Institute of Technology and Advanced Learning. He received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Federal University of Para (UFPA), Brazil, in 1999, 2001, and 2005, respectively. He worked as a Professor at UFPA from 2005 to 2015, Department of Computer Science where he served as a Chair of the Faculty of Information Systems (2005–07) and Vice-Chair of the Graduate Program in Computer Science (2010–12). From 2010 to 2015 he served as an Associate Editor of the Computers and Electrical Engineering (CAEE)-Elsevier where he was a Top Associate Editor in 2011. He was a Guest Editor for the CAEE special issue on the Design and Analysis of Wireless Systems: New Inspirations. He worked as a Postdoctoral Fellow (PDF) and Instructor at Ryerson University, Department of Computer Science and served as the Chair of the IEEE Toronto Section Signals & Computational Intelligence Joint Society (2016). Dr. Carvalho's research interests include security and performance analysis of cloud systems, distributed systems, and 5G wireless networks.

Ahmed S. Khwaja received the B.Sc. degree in electronic engineering from the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Pakistan, and the Ph.D. and M.Sc. degrees in signal processing and telecommunications from the University of Rennes 1, France. He is currently a Senior Research Associate with the WINCORE Lab. His research interests include machine learning, compressed sensing, remote sensing, and optimization problems in wireless communication systems and smart grid.

Ling Guan is a Professor of Electrical and Computer Engineering at Ryerson University, Toronto, Canada, and a Tier I Canada Research Chair in Multimedia and Computer Technology. He held visiting positions at British Telecom (1994), Tokyo Institute of Technology (1999), Princeton University (2000), National ICT Australia (2007), Nanyang Technological University (2007), Hong Kong Polytechnic University (2008–09), Microsoft Research Asia (2002, 2009, 2017) and Chinese Academy of Science (2010). Dr. Guan has published extensively in multimedia processing and communications, human-centered computing, machine learning, adaptive image and signal processing, and, more recently, multimedia computing in immersive environment. He is a Fellow of [illegible] Elected Member of the Canadian Academy of En[illegible]ering, a[illegible] IEEE Circuits and System Society Distinguishe[illegible] Lecturer. Dr. [illegible] has been honored with numerous [illegible]ards, including the [illegible]4 IEEE Canada C.C. Gotlieb Medal fo[illegible]hnical Achievement [illegible] Computer Science and Engineering, a[illegible] 2005 IEEE Tra[illegible]ctions on Circuits and Systems Best Paper A[illegible]. Dr. Gua[illegible]ceived his B.Sc. Degree from Ti[illegible]n University, M[illegible] Deg[illegible] from University of Waterloo, [illegible] Ph.D. Degree from th[illegible]ersity of British Columbia.

Is[illegible]oungang r[illegible]ved his M.A.Sc. and Ph.D. degrees in Mathe[illegible]ics from [illegible] University of Aix Marseille II and University o[illegible]th[illegible]oulon and Var, France, in 1990 and 1994 respectively. [illegible]999, he received a M.A.Sc from INRS-EMT, University of Quebec in Montreal, Canada. From 1999 to 2002, he worked as a Software engineer at Nortel Networks. [illegible] 2002, he has been with the Department of Computer Sci[illegible]t Ryerson University, where he is now a Full Professor. During his sabbatical, he was a Visiting Professor at Fukuoka Institute of Technology (FIT), Japan. In 2004, he founded the Distributed Applications and Broadband NEtworks Laboratory (DABNEL). His research interests includes network security, radio resource management in next generation networks, IoT and cloud systems. Dr. Woungang serves as Co-Editor in Chief of the International Journal of Communication Networks and Distributed Systems (IJCNDS), Inderscience, UK, Associate Editor of the International Journal of Communication Systems (IJCS), Wiley. Dr. Woungang has edited several books in the areas of networks and pervasive computing, published by reputed publishers such as Springer, Elsevier, and Wiley.