COMPUTERS & SECURITY 68 (2017) 81–97

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Cyber physical systems security: Analysis, challenges and solutions

Yosef Ashibani *, *Qusay H. Mahmoud*

Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada

ARTICLE INFO

Article history:
Received 28 October 2016
Received in revised form 5 April 2017
Accepted 7 April 2017
Available online 12 April 2017

Keywords:
Cyber Physical Systems (CPS)
Internet of Things (IoT)
CPS security analysis
Risk assessment
Security architecture
Research challenges

ABSTRACT

Cyber Physical Systems (CPS) are networked systems of cyber (computation and communication) and physical (sensors and actuators) components that interact in a feedback loop with the possible help of human intervention, interaction and utilization. These systems will empower our critical infrastructure and have the potential to significantly impact our daily lives as they form the basis for emerging and future smart services. On the other hand, the increased use of CPS brings more threats that could have major consequences for users. Security problems in this area have become a global issue, thus, designing robust, secure and efficient CPS is an active area of research. Security issues are not new, but advances in technology make it necessary to develop new approaches to protect data against undesired consequences. New threats will continue to be exploited and cyber-attacks will continue to emerge, hence the need for new methods to protect CPS. This paper presents an analysis of the security issues at the various layers of CPS architecture, risk assessment and techniques for securing CPS. Finally, challenges, areas for future research and possible solutions are presented and discussed.

1. Introduction

Cyber physical systems (CPS) are a combination of closely integrated physical processes, networking and computation. The physical process is monitored and controlled by embedded (cyber) subsystems via networked systems with feedback loops to change their behavior when needed (Asare et al., 2012). These subsystems work independently of each other with the ability to interact with the external environment (Ali et al., 2015; Wang et al., 2010). The physical processes are achieved by several tiny devices with sensing, computing and communication (often wireless) capabilities. These physical devices can be identified with physical attributes or information sensing equipment, such as infrared sensors or Radio Frequency Identification (RFID), and can then be connected to a networking system, in most cases the Internet, to send the captured data to the computational subsystem (Zhang et al., 2011).

With the increased focus on data handling capacity, data communications capability and integration of information systems, as well as physical devices, the demand for integrating CPS in different fields is also increasing, resulting in widely gained attention not only from universities and research and development labs but also from industry and government agencies (Lu et al., 2015). Prior to the current form, CPS evolved through different stages: Embedded Systems, Intelligent Embedded Systems and Systems of Systems (Sendler, 2013). The

* *Corresponding author.*
E-mail addresses: yosef.ashibani@uoit.net (Y. Ashibani), qusay.mahmoud@uoit.net (Q.H. Mahmoud).
http://dx.doi.org/10.1016/j.cose.2017.04.005
0167-4048/

current form of CPS is used in many different areas such as the power, petroleum, water industry, chemical engineering, healthcare, manufacturing, transportation, automotive systems, entertainment, consumer appliances, in addition to many other areas that are directly related to people's daily lives. It was estimated that cyber physical components would account for 40% of an automobile's total value by the end of 2015 (NIST, 2012), and that in 2020, around 25 billion uniquely identified objects will be used (Jing et al., 2014).

CPS have many features, such as enabling individual components to work jointly, producing complex systems (Vegh and Miclea, 2014). In CPS, data can be captured by physical objects or sensor devices, and transferred through networks to the control system with the absence, in some cases, of any human to machine interaction (Bhabad and Scholar, 2015). The physical objects are increasingly equipped with, for example, infrared sensors, barcodes or RFID tags which can be scanned by smart devices (Khan et al., 2012). These devices can be connected to the Internet to send the identified data and location placement to be used for monitoring and managing the physical environment (Zhang et al., 2011). The computational and processing units can also be placed in the cloud, with the resulting decisions issued as actions to the physical objects (Khan et al., 2012). As an example of CPS, Industrial Control Systems (ICS) are isolated by communication protocols and operating systems from the outer systems. For the time being, these kinds of systems are increasingly interrelated through the Internet in improving functionality and automation. The increased connectivity of the cyber and physical world brings significant security challenges to the CPS (Shafi, 2012). As the importance of these systems is in improving functionality, the interconnectivity among CPS subsystems is growing (Peng et al., 2013).

Security concerns ranging from application environment and communication technology should be addressed at the early stages of the design (Gamundani, 2015). Moreover, the inherent characteristics and advantages of using available networks, such as Wireless Sensor Networks (WSN), Next-Generation Networks and the Internet, CPS are increasingly facing new security challenges, such as securing protocols and establishing trust between CPS subsystems (Lu et al., 2013). Many of the computing subsystems in CPS are based on commercial-off-the-shelf (COTS) components. The COTS components provide a significant level of control, lower deployment, and lower operational costs in comparison to the traditional vendor specific proprietary and closed-source systems. However, this exposes CPS to more vulnerabilities and threats (Nourian and Madnick, 2014). As an example, industrial control systems have been considered secure when not connected to the outside world (Nourian and Madnick, 2014), without taking into account insider attacks. Thus, this indicates that the extensive connectivity between cyber and physical components raises the important issue of security.

More attacks are expected as many interactions among different components are connected outside of their area to provide better services, such as Smart Grid networks. For example, in the field of the power industry, a power plant monitoring system was attacked in 2010. Consequently, a 900MW load was lost in under 7 seconds. In the energy sector, the Iran Bushehr Nuclear Power Plant computer system was attacked by "Stuxnet" in the same year, which led to severe disorder in the nuclear facilities' automated operations and a serious deterioration in Iran's nuclear program (Peng et al., 2013). According to a CIA report, power systems in several regions outside the United States have been penetrated by attackers, leading to power outage in multiple cities. In the medical field, implanted human medical devices have been attacked by hackers through their wireless communications (Leavitt, 2010).

In the transportation field, an exception in the management system of Japan's control schedule resulted in five Shinkansen operation management system failures. Consequently, 124 trains were delayed while 15 trains were suspended, affecting the travel of 8.12 million people (Peng et al., 2013). It has been demonstrated that airplanes could be controlled by attackers via accessing built-in Wi-Fi services (Nourian and Madnick, 2014). In 2010, CarShark was invented, a software with the ability to remotely turn off a car's engine and brakes leading to a loss of control to stop the car. This software was also able to monitor communications between electronic units, providing incorrect readings, and inputting false data to perform the attack. Meanwhile, in that same year, other attackers succeeded in creating a new virus to attack the Siemens plant control system (Wang et al., 2010).

These security incidents provide enough evidence that attacks on CPS, in particular on the cyber layer, can lead to a great loss in people's livelihoods. Therefore, CPS security is becoming more important than ever and should be taken into consideration in the early stage of the design process. Moreover, advanced CPS security techniques are needed to increase the protection of these increasingly complex interconnected systems (Jalali, 2009). Most of the efforts in security solutions were based on the available solutions designed specifically for classical Information Technology (IT) systems to develop or create advanced solutions. However, these solutions are not designed for CPS (Konstantinou et al., 2015; Wang et al., 2010). Additionally, most of the research focuses on the performance, stability, robustness and efficiency of physical systems rather than security, which is broadly ignored, usually as a result of constrained factors, such as low processing, communication and adequate storage ability capacities. However, if security is disregarded, CPS will not work in a stable manner (Lu et al., 2014). In response to the real need to apply security methods to protect these interconnections, a tight coupling in the interconnections between physical and cyber controlling components is required. Security issues are not new; however, advances in technology make it necessary to produce new approaches to protect data from hazards (Nourian and Madnick, 2014). Additionally, CPS privacy is another serious issue that should be taken into consideration (Lu et al., 2014) in any proposed security solution.

1.1. *Contributions*

Several papers in the literature discuss CPS security and focus only on particular issues. For example, the focus in Neuman (2009) is on the physical control of the CPS, and the author offers some suggestions for protecting communication channels, real-time requirements and applications. In Lu et al. (2014), a security framework for CPS is proposed with a comprehensive analy-

sis regarding three aspects of security objectives: security in specific, CPS applications and security approaches. However, it does not consider all aspects of security, such as authenticity which is the most important security objective of CPS. The authors in Alvaro et al. (2009) discuss the important challenges that CPS face and provide an analysis of threats and possible attack consequences, as well as explain the differences between traditional IT security and CPS. Even though this study provides a significant discussion, its focus is on developing adversary models of CPS, especially for protecting control systems.

To this end, this paper presents analysis of security issues in CPS with a brief overview of the system level architecture and its components. The contributions of this paper are:

- A state-of-the-art review, an analysis and comparison of security issues for CPS utilizing three-level architecture based on the respective functions of each layer.
- A comparison between CPS security and traditional IT security focusing on distinguishing characteristics, risk assessment and possible attacks at each layer.
- An analysis of CPS security requirements and challenges, a discussion of possible solutions and areas for future research.

The rest of this paper is organized as follows. Section 2 presents Cyber Physical Systems (CPS), differences with the IoT and architecture models. Distinguishing characteristics of CPS and security issues are presented in Section 3. Section 4 provides an analysis of the security issues at the various layers of CPS architecture. Possible CPS security solutions are presented in Section 5 while a discussion and ideas for future research areas are covered in Section 6. Finally, Section 7 concludes the paper with a summary of the findings.

2. Cyber-physical systems

As computing devices have become lightweight, portable, and capable of being connected with the real world, CPS components can be interconnected through the Internet with the capability of system monitoring and controlling with proper operation and real-time response. CPS provide a coupled environment that contains interconnectivity of thousands of devices, providing more convenience in management and control.

2.1. *CPS vs. IoT*

More recently, the terms CPS and Internet of Things (IoT) have been used interchangeably due to the large gray area of overlap between them. We have observed that academic institutions prefer CPS whereas government agencies and the industry prefer IoT (Gładysz, 2015; Soldatos, 2015). However, some researchers in big data analytics also use the term IoT. In general, IoT is defined as a communication network connecting things which have naming, sensing and processing abilities (Chen, 2010). In addition, IoT enables loosely coupled decentralized systems of cooperating smart objects, which may act as intelligent agents that exchange information with users through transmission media, such as WSN (Kumar and Patel, 2014). Interconnectivity among such smart objects, including devices, actuators, sensors, embedded computers and RFID tags, is in most cases based on standard communication protocols such as Bluetooth, RFID, 6LoWPAN and ZigBee (Chang et al., 2015; Soldatos, 2015).

The term CPS, on the other hand, is mainly related to real-time systems including distributed real-time control systems that integrate computing and communication capabilities with monitoring and control of entities in the physical world (Suo et al., 2012). CPS have also been defined in terms of control systems with real-time capabilities and distributed networks with minimal human interaction (Peng et al., 2013). Furthermore, CPS are referred to as the next generation of embedded intelligent information and communications technology systems, which are interdependent and collaborative. This provides computation, communication and monitoring/control of physical component processes in various applications (Vermesan and Roy, 2016), such as aerospace, transportation, energy, healthcare and manufacturing. Moreover, CPS are found in many fields that require real-time data collection and feedback decision making including nano-level manufacturing, robotic surgery, air traffic control, military combat, firefighting and deep-sea exploration (Chang et al., 2015; Soldatos, 2015).

2.2. *CPS architecture*

The modern definition of CPS is the integration of computing, communication, and control capabilities that monitor and control the objects in the physical world. The physical processes are controlled and monitored by cyber systems (Shafi, 2012), which are embedded computers and networks with feedback loops. The computations will be affected by the physical processes and vice versa (Miclea and Sanislav, 2011).

Although there is a global unanimity in defining the CPS, there is no consensus on the essential parts of the CPS and their communication models (La and Kim, 2010). The CPS architecture commonly referred to two main layers, the physical and cyber. The physical layer captures sensed data and performs the cyber layer commands, whereas the cyber layer analyzes and processes the physical layer data and releases the appropriate commands accordingly (Lu et al., 2015).

As discussed in Wu et al. (2010), not all of the features of the CPS will be distinguished by a three-layer structure. However, new CPS architectures have been proposed, some of which are non-hierarchical with unclear descriptions (Lu et al., 2015). Considering the different factors, such as reliability coordination, service composition, service management and object abstraction, that need to be addressed, more than three layers of architecture have been proposed, as in Khan et al. (2012), Suo et al. (2012), and Zhang et al. (2011). Considering that the CPS need to be managed and controlled, the structure should have more stages and details. In addition, taking into account the various developments that have been implemented, a new architecture has been updated, as in Wu et al. (2010) which comes with five layers: business, application, processing, transmission and perception. Even though there are different assumptions about the number of layers, CPS fundamentally operates at three layers: perception, transmission and appli-

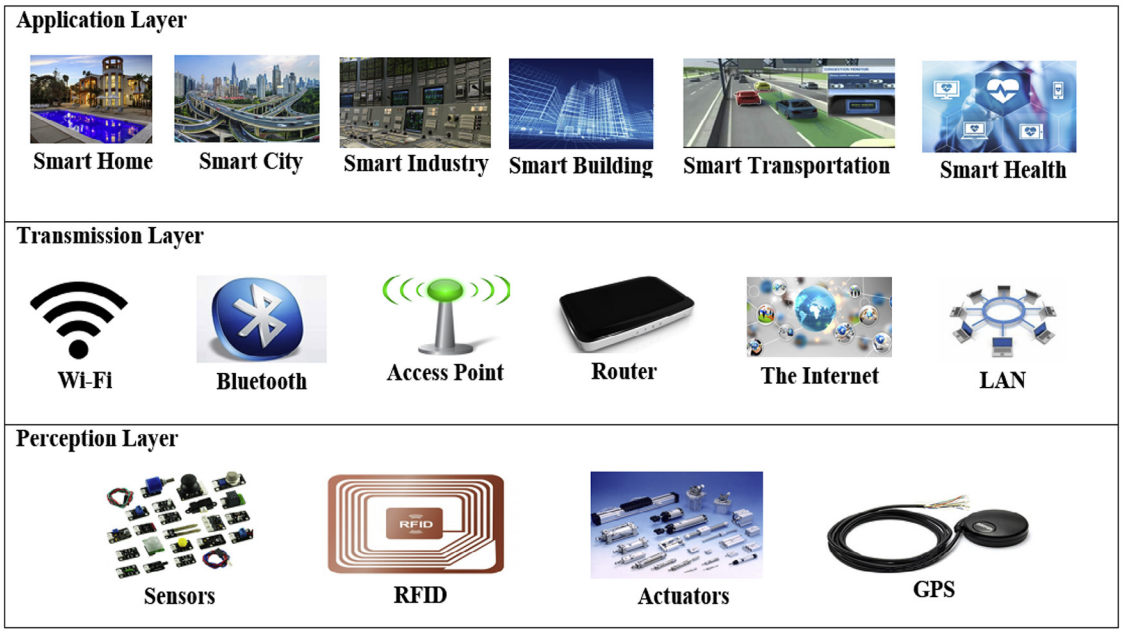

Fig. 1 – Typical three layers cyber-physical system.

cation (Gou et al., 2013; Mahmoud et al., 2015; Peng et al., 2013; Zhao and Ge, 2013). Each of these layers is defined by the devices within it and the related functions that should be implemented (Ashok et al., 2011; La and Kim, 2010). Based on the achieved functions at each layer, this paper considers a three-level CPS architecture as shown in Fig. 1: perception (physical) layer, data transmission (network) layer, and application (cyber) layer.

The first layer is the perception layer, also called the recognition layer (Kumar and Patel, 2014) or sensors layer (Mahmoud et al., 2015). This layer has multiple terminal equipment such as sensors, actuators, cameras, Global Position Systems (GPSs), laser scanners, intelligent devices, RFID tags with 2-D bar code labels and readers (Lu et al., 2015; Wu et al., 2010; Zhang et al., 2011). Devices at this layer have the ability to collect real-time data that is needed for different purposes (e.g. monitoring and tracking), interpret what they receive from the physical world and perform commands from the application layer. The collected data can include sound, light, mechanics, chemistry, heat, electricity, biology or location (Peng et al., 2013; Zhao and Ge, 2013). Sensors can generate real-time data with node cooperation in wide and local network domains (Mahmoud et al., 2015), which will be aggregated and analyzed in the application layer. Sensors, depending on their type, can aggregate information related to temperature, acceleration, humidity, vibration, location or air chemical changes (Khan et al., 2012).

The second layer is the transmission layer (also known as the transport layer (Lu et al., 2015) or network layer (Khan et al., 2012)), which is responsible for interchanging and processing data between the perception and the application. The data interaction and transmission in this layer are achieved using local area networks, communication networks, the Internet or other existing networks through many technologies such as Bluetooth, 4G and 5G, UMTS, Wi-Fi, Infrared and ZigBee, depending on the sensor devices (Khan et al., 2012). However, most of the interconnections are achieved via the Internet for many reasons, including availability and cost effectiveness. This means that real-time operations should be supported by the used networks. As it is important to manage and process massive data, the transmission layer can initially process and manage a vast amount of data and realize real-time transmission (Lu et al., 2015) with responsibility for reliable communication support (Zhang et al., 2011).

Many protocols and functions can be found at this layer for the purpose of addressing an increased number of objects such as Internet Protocol version 6 (IPv6) (Wu et al., 2010). Furthermore, the function of this layer includes data routing and transmission through various devices and hubs over the used networks (Mahmoud et al., 2015). Cloud computing platforms, routing devices, switching and Internet Gateways work as well at this layer using technologies such as Wi-Fi, LTE, Bluetooth, 4G/5G or ZigBee. The network Gateway serves as the connector point of different nodes that collects, filters, transmits and receives data among the nodes (Mahmoud et al., 2015) and other layers of the CPS. The increased number of connected devices poses another issue in CPS, which is traffic and storage (Khan et al., 2012). This will affect security within the CPS. Although this traffic can be managed by protocols including firewalls, the security of devices with limited capabilities cannot be guaranteed since their computational capabilities and storage are very limited (Mahmoud et al., 2015).

The third and most interactive layer is the application layer. Its mission is to process the received information from the data transmission level and issue commands to be executed by the physical units, sensors and actuators (Peng et al., 2013). This layer works by implementing complex decision-making algorithms on the aggregated data to generate correct decisions (Ali et al., 2015), and control commands which will be used in corrective actions. In addition, this layer receives and pro-

cesses information from the perception layer and then determines the required automated actions to be invoked (Khan et al., 2012). Data aggregation from different resources and intelligent processing of massive data are performed at this layer with object control and management. Cloud computing, middleware, and data mining algorithms can also be used in management implementation of connected devices at the physical layer (Zhang et al., 2011).

Monitoring of the system is also performed here in this layer and its mission is to observe the behavior of physical processes, and issue commands to change the behavior of physical devices to ensure the work environment functions both correctly and optimally. The application layer also saves past actions so that feedback of any previous action can be given for ensuring future operational improvements. The objective of this layer is to create a smart environment (Mahmoud et al., 2015), and combine CPS and industry professional applications. This has led to extensive and intelligent applications in areas that may include private and secure data, such as: Smart Power Grid; Smart Homes and Cities; Intelligent Transportation (Peng et al., 2013); Smart Auto; environmental monitoring; industry control (Lu et al., 2015), Smart Health; and Smart Farming. Such applications might collect users' private data, such as health information and habits. Therefore, it is important to apply mechanisms to protect the data. On the other hand, application systems are different and require appropriate security policies. Hence, it is difficult to individually address a security policy for each application system. As the use of CPS is increasing, security challenges are also increasing and need to be considered.

3. CPS security

In general, the security in CPS is classified into two areas: information (data) security and control security. Information security involves securing information during data aggregation, processing and large-scale sharing in the network environment, especially open loosely coupled networks. Control security encompasses resolving any control issues in the network environment and mitigating the control system from any attacks on system estimation and control algorithms (Cárdenas et al., 2011; Lu et al., 2013). Information security focuses on data protection, for example by using encryption, whereas control security focuses on protecting the dynamics of control systems against cyber-attacks (Lu et al., 2015). The sole focus of the remainder of this paper is on information security. In addition to discussing the distinguishing characteristics between CPS and traditional IT systems, this section presents an analysis of the most important security factors, objectives, attacks and risk assessments for CPS.

3.1. *Distinguishing characteristics*

In IT systems, access restriction and control can be applied without affecting the system services. On the other hand, any IT protection measures applied for CPS could affect or delay the real-time response of the physical parts of CPS which usually demand real-time responses. For example, the main risk factors for ICS are consolidated technologies, unified protocols, expanded connectivity, and public information access, which mostly result in insecure connections (Stouffer et al., 2011). Thus, applying IT strategies for CPS may unfortunately affect real-time responses and provide potential adversaries with many new opportunities to disrupt the services provided by the CPS. However, due to the unique characteristics of the CPS, traditional IT security strategies and approaches are not sufficient for addressing CPS security challenges due to the differences in specifications and connectivity from CPS (Nourian and Madnick, 2014).

In addition to the three security objectives of traditional IT systems, authenticity is considered as the fourth CPS security objective. Authenticity indicates that all transactions and communications must be guaranteed that are between legitimate parties (Shafi, 2012) in all related processes such as sensing, communication, or actuation (Wang et al., 2010), hence ensuring that the source of any action that highly impacts the system was originated and issued from a trusted party (Wood and Stankovic, 2010). In other words, authenticity for CPS seeks to validate both communicated parties and authenticate and verify any related process (Wang et al., 2010). Though confidentiality is ranked the first security objective for IT systems, availability comes first for CPS, then integrity, confidentiality and authenticity. However, authenticity should be ranked first as other security objectives are built on it, and any failure to ensure that the right parties are who they claim to be will mean that other security goals will be useless. For example, if an unauthorized (e.g. malicious) party successfully accessed the system, confidential information will be released, and the integrity will not be satisfied since such a party can manipulate information. Since, in most cases, there will be no human interaction to ensure the authentication process of the connected objects, a robust authentication mechanism must be included to protect the system and make the correct decisions for accepting or rejecting the received instructions and data (Shipley, 2013). Thus, the most important security factor in CPS is how to ensure proper access control to the system, known as identity-based in traditional IT security (Kirkpatrick et al., 2009).

Another difference between IT and CPS is that traditional security techniques individually focus on addressing security for system components rather than the interactions among these components. Hence, the main goal is addressing safety (absence of failure) issues rather than security (unauthorized access). To some extent, security and safety analysis and solutions of complex systems can be provided by traditional techniques. However, new issues in such systems, such as network heterogeneity, different component interactions, and cyber connections are not successfully considered. An example of such an issue is that a control parameter can be modified as a reason of unsuccessful authentication process. Thus, a security attack happens without failure incidence in the system (Nourian and Madnick, 2014). Hence, in some cases, a system cannot be considered secure with the absence of failure. As a result, applying traditional security techniques to CPS will not fully protect against attacks. Hence, the prime security challenge is the need to consider interactions among CPS components.

Although the three IT security objectives (confidentiality, integrity and availability) are necessary for CPS, they are not sufficient by themselves. If a cyber-system is not accessible, the physical processes will not be controlled, and the consequences will be catastrophic (Lu et al., 2013), particularly for real-time operations. For example, without a proper confidentiality mechanism, secret data might be captured by an unauthorized party; without an appropriate integrity mechanism, critical data may lead to deception through false data; without adequate availability, the system might not be accessible when needed (Lu et al., 2014); without an authenticity mechanism, received data might be sent from an attacker or originated and issued from an unknown party. These four objectives are the four basic security goals of CPS.

As CPS perform different processes at various stages and securing devices, data transmissions, applications and data storages and actuation processes are required. The following subsections briefly describe these requirements.

3.1.1. *Securing access to devices*

Securing access to devices becomes the first challenge. If authentication is not or is poorly supported, unauthorized objects will gain access and manipulate the system (Konstantinou et al., 2015), hence, neither trusting any underlying binary codes, nor implementation at the application layers will be guaranteed.

3.1.2. *Securing data transmissions*

Data transmission security is required in order to detect impostors and malicious activities in CPS communication networks and block unauthorized access. As an example, attackers try to intercept the physical properties of system power consumption and timing behaviors to analyze the data being sent and received (Konstantinou et al., 2015). Some attackers aim to disrupt networks by launching DoS attacks or interrupting the routing topology (Raza, 2013).

Some terminal devices, which are not a complete computer system, do not have high data processing and communication abilities, or adequate storage capacities (Wang et al., 2010). This makes these devices more vulnerable to penetration. On the other hand, in Industrial Control System terminals, connectivity, which relies on open networking standards, helps to improve system performance and reduces operational costs. Although such terminals lead to more efficient and effective operation, they expose the system to higher possibilities of intrusions and malicious attacks, such as malicious code (malware), distributed denial of service (DDoS), eavesdropping and unauthorized access (Weiss, 2010). Another factor which directly leads to vulnerabilities is that the designing process is always constrained in processing time (speed), hardware resources and power consumption. Moreover, embedded systems are designed by experts who have limited experience of security issues, and focus more on functionality, error corrections and performance than security (Hu et al., 2013). This, in turn, leads to vulnerabilities in the system, which may leak secure information to unauthorized or undesired users.

3.1.3. *Securing applications*

The application layer combines different applications and security challenges. Privacy protection matters faced at this layer will not be addressed in the other layers where some security challenges do not occur. Here, the private information of users can be analyzed by attackers, leading to private data leakage and privacy loss. Since this data might contain past and present locations that the users visited, some data protection techniques regarding data protection at this layer include location camouflage, anonymous space or space encryption. In addition, many applications in this layer apply to users' social life, therefore need to be protected (Jing et al., 2014).

3.1.4. *Securing data storage*

Protecting stored secret data in CPS devices is important. Most CPS devices, such as sensors, are tiny, wirelessly connected and resource-constrained nodes (Raza, 2013). Although various software based solutions use cryptographic techniques to encrypt data in such devices, they are not sufficient due to the constraints of memory and weak processing capabilities of these devices. As a result, lightweight security mechanisms are required (Lu et al., 2013).

3.1.5. *Securing actuation*

Actuation security means that any actuation actions must be issued from authorized sources. This will ensure that the provided feedback and control commands are correct and protected against adversaries (Wang et al., 2010).

As a result of using the Internet as a transmission layer in CPS connections, Internet security issues will also be involved. In general, security should be implemented for the entire system as one end-to-end security scheme rather than for only the operating security mechanism at each layer (Jing et al., 2014). Moreover, heavyweight computations and large memory requirements are currently the primary requirement of any desired security solution (Stankovic, 2014).

3.2. *Attacks on CPS*

Attacks on CPS could result in severe damage to the physical environment. Each layer of CPS is susceptible to either passive or active attacks. Furthermore, CPS is vulnerable to more attacks than traditional IT systems, which are not limited to CPS, but to attacks from the used network, especially the Internet (Peng et al., 2013), which is already employed as the transmission layer. Perception layer attacks, for example, include attacks on nodes such as sensors and actuators; transmission layer attacks include data leakage or damage and security issues during data transmission; application layer attacks include unauthorized access leading to loss of user privacy (Lu et al., 2015). Thus, analyzing possible attacks and building a robust security architecture are required. Although each layer is susceptible to different attacks, some attacks could target all layers, and according to Gou et al. (2013), Lu et al. (2015), Mitchell and Chen (2014), Peng et al. (2013), Raza (2013), Suo et al. (2012), and Zhao and Ge (2013), examples of these attacks include:

- Denial of Service (DoS): Alters behavior characteristics by blocking traffic to make the network and the service unavailable by, for example, flooding a resource with false requests, taking advantage of protocol vulnerability. Moreover, DDoS is a common attack that targets multiple

resources, such as the end devices and the network, at the same time, preventing access to information and services (Ali et al., 2015; Zhao and Ge, 2013).

- Man-in-the-Middle (MITM): Sends a fabricated message to a targeted resource which accordingly takes undesired actions by, for example, controlling a primary function, based on the received message which could cause an undesirable event. The network layer is also vulnerable to this type of attack which, in some cases, is followed by eavesdropping (Ali et al., 2015; Mahmoud et al., 2015; Shafi, 2012).
- Eavesdropping: Intercepts any transferred data by the system. For example, transmitting control information for monitoring purposes in the CPS from sensor networks to the applications could become susceptible to eavesdropping. Additionally, user privacy could also be breached as the system is being monitored (Kao and Marculescu, 2006; Shafi, 2012).
- Spoofing: Pretends to be a legitimate part of the system, then attempts to be involved in system activities. After achieving successful access, the attacker will have access to information and can perform any operation such as modifying, deleting or inserting information (Shafi, 2012).
- Replay (playback): Retransmits a received packet from the destination node, to attain the trust of the system (Zhao and Ge, 2013). This type of attack can be launched by spoofing and altering or replying the identity information of one of the devices (Mahmoud et al., 2015).
- Compromised Key: Targets the secret key which is being used for securing communication. This can be achieved by analyzing the required encryption time, also known as timing (side channel) attack (Mahmoud et al., 2015; Zhao and Ge, 2013). The compromised key will then be used to modify captured data and perform computational analysis to compromise other secret keys in the same system. In some cases, an adversary could obtain access to sensors and force them to perform engineering tasks to extract other inside keys. In another example, an attacker could succeed in replacing a sensor node and pertain as the legitimate version to exchange keys with other nodes (Ali et al., 2015; Raza, 2013; Wang et al., 2010), thereby, discovering other secret keys of the involved nodes.

There are different kinds of risks at each level of the CPS, and based on the CPS architecture shown in Fig. 1, common attacks for each layer can be classified as follows.

3.2.1. *Attacks at the perception layer*

The perception layer consists of end devices, such as tags in RFID and sensors, which are limited by the constrained computing resources and memory capabilities. In addition, these devices are mostly located in external and outdoor environments, resulting in physical attacks, such as tampering with the devices' components or replacing the devices. Hence, those terminal devices are most susceptible to a variety of attacks (Shafi, 2012). Common attacks at the perception layer include equipment failure, line failure, witch, electromagnetic interference, perceptual data corruption (Peng et al., 2013), differential power analysis (Zhao and Ge, 2013), information disclosure, information tracking, tampering, sensing information leakage (Gou et al., 2013), physical destruction and energy-exhaustion attacks (Bhattacharya, 2013). Common forms of these attacks are:

- Node Capture: Takes over the node and attains and leaks information that could involve encryption keys, which is then used to threaten the security of the entire system. This kind of attack targets confidentiality, availability, integrity and authenticity (Bhattacharya, 2013; Mahmoud et al., 2015; Zhao and Ge, 2013).
- False Node: Adds another node to the network, attacking data integrity by sending malicious data. This, in turn, might lead to a DoS attack, by consuming the energy of the nodes in the system (Mahmoud et al., 2015; Zhao and Ge, 2013).
- Node Outage: Stops nodes services, making it difficult to read and gather information from these nodes, as well as launches a variety of other attacks which affect the availability and integrity (Bhattacharya, 2013).
- Path-Based DOS: Sends a large number of packets, flooding packets, along the routing path to the base station, leading to battery exhaustion of the node and network disruption, consequently reducing the availability of the nodes (Bhattacharya, 2013).
- Resonance: Forces compromised sensors or controllers to operate at a different resonant frequency (Alvaro et al., 2009).
- Integrity: Tries to inject external control inputs and false sensor measurements, wishing to disrupt the system (Ali et al., 2015; Mo and Sinopoli, 2012).

3.2.2. *Attacks at the transmission layer*

Attacks on this layer are in the form of data leakage during the information transmission. This occurs as a result of the openness of the transmission media, especially in wireless communication. Such attacks capture a transmitted message through radio interface, modify and retransmit it, or exchange information between heterogeneous networks, hence impersonating the legitimate user. Also, other factors, such as remote access mechanisms among massive amounts of network nodes that could cause traffic congestion, would increase the chance of being attacked (Mahmoud et al., 2015; Peng et al., 2013; Shafi, 2012). Common attacks at this layer include response and Sybil, traffic analysis, tampering, exhaustion, collision, black hole, flooding, trap doors, sink node, direction misleading sinkhole, wormhole, wrong path selection, tunneling (Peng et al., 2013; Raza, 2013) and illegal access (Gou et al., 2013; Mitchell and Chen, 2014). The following examples are common forms of attacks at the transmission layer:

- Routing: Creates routing loops that may result in resistant network transmission, increased transmitting delay or extended source path (Raza, 2013; Zhao and Ge, 2013).
- Wormhole: Makes information holes in the network by announcing false paths through which all the packets are routed (Gaddam et al., 2008).
- Jamming: Jams the wireless channel between sensor nodes and the remote base station to introduce noise or a signal with the same frequency. This attack could lead to DoS by creating intentional network interference (Li et al., 2013; Maheshwari, 2016; Raza, 2013).
- Selective Forwarding: Makes a compromised node to drop and discard packets, and forward selected packets. In some

cases, the compromised node stops forwarding packets to the intended destination or only forwards chosen messages and discards all other packets while this node is considered as legitimate (Raza, 2013).
- Sinkhole: Announces the best routing path to be used to route the traffic to other nodes. This attack could be used to launch other attacks, such as selective forwarding and spoofing (Raza, 2013).

3.2.3. *Attacks at the application layer*

As a large amount of users' information is gathered at this layer, attacks here result in data damage, privacy loss such as user habits and health conditions, and unauthorized access to devices (Peng et al., 2013). Common attacks at the application layer include user privacy leakage, unauthorized access, malicious code, database and control command forgery attacks (Lu et al., 2015; Peng et al., 2013; Suo et al., 2012). Common examples of attacks at this layer include:

- Buffer Overflow: Takes advantage of any vulnerabilities in the software that lead to buffer overflow vulnerabilities and exploit it to launch attacks (Zhao and Ge, 2013).
- Malicious Code: Attacks the user application by launching various malicious codes, such as viruses and worms, and causes the network to slow down or cause damage (Suo et al., 2012).

3.3. *Risk assessment*

With increased CPS usage in many sensitive fields (e.g. Medical Healthcare and Smart Homes), security has become an urgent issue and poses a need for an adequate risk assessment method (Lu et al., 2013). The security focus of risk assessment has transferred from computer risk assessment to network risk assessment, especially with extensive dependence on the Internet (Peng et al., 2013). The goal of assessing CPS security is to have a quantified form of risk that can be employed in future system protection. However, most of the efforts and studies focus on the enterprise systems which are not directly related to CPS (Zalewski et al., 2013). Since CPS security, to a great extent, is different from traditional IT systems, the security features are also different. For example, standardized protocols and technologies, insecure interconnections and interchanged information are the main risk factors for ICS (Stouffer et al., 2011). The CPS risk assessment model can be divided into three steps: (1) defining what will happen to the system; (2) evaluating the probability of the event; and (3) estimating the consequences. Furthermore, three elements should be taken into account when making CPS risk assessment: asset (value), threat and vulnerability identifications (Lu et al., 2013).

3.3.1. *Asset identification*

An asset, which refers to a resource value that needs to be protected (Gamundani, 2015), can be a tangible presence (e.g. medical devices, business facilities, equipment activities, educational facilities, operations, or information) or an intangible presence (e.g. information about a company, or reputation of an association). In fact, most assets are intangible; thus, assets have a direct value for many daily transactions and services and so should be protected. Additionally, asset quantization can be estimated from direct and indirect economic losses and the resulting damage (Stouffer et al., 2011). The value assessment process includes identifying the defense layers, critical assets, and the core (essential) functions of the system, as well as determining the asset value rating (Moteff, 2005). CPS assets can be divided into three parts: physical assets, cyber assets and interactions with other systems. The essential difference between CPS assets and classical IT assets is that the intercommunications of CPS are complex, intangible and interconnected with other systems.

3.3.2. *Threat identification*

This step is used to help identify risks that are a high priority concern in the field of CPS, which is not an easy mission. Historical data can be used to quantify the frequency of the threat while sampling records and logs in the Intrusion Detection System (IDS) can be used to determine the frequency of the risk, logs and many other methods (Lu et al., 2013). IDS techniques are out of the scope of this paper, however, Mitchell and Chen (2014) present a comprehensive literature review that classifies new CPS IDS techniques, presents research directions, and summarizes the most studied CPS IDS techniques in the field.

3.3.3. *Vulnerability identification*

Vulnerability is defined as any existing weakness that could be exploited for spying purposes by an adversary to eavesdrop on or harm the value of an asset. It is also defined as a condition or environment that can be exploited by an adversary to assault or damage systems (Lu et al., 2013). A vulnerability assessment is an analysis process of a system and its functions, identifying weaknesses and determining appropriate corrective actions or mitigations that could be designed and implemented to reduce or eliminate any vulnerabilities (Moteff, 2005).

CPS vulnerabilities are generally divided into three: network, platform and management. Network vulnerability involves configuration, hardware and monitoring vulnerabilities (Lu et al., 2013). Platform vulnerability includes configuration, hardware and software vulnerabilities as well as deficiency of protection measures. Management vulnerability is most related to the lack of security policies. Vulnerability quantization can be obtained through a different mechanism such as the previous expert evaluating methods, comparing with historical records or best experiences in industries (Gamundani, 2015). Eliminating or preventing all risks is a difficult mission, if not close to impossible. Accordingly, least cost methods are usually adopted to reduce the risks to an acceptable level.

4. CPS security analysis

As CPS combine cyber and physical processes, there is an increase in the number of challenges that CPS should be considered when designing a security mechanism for such systems. Furthermore, the environment is continuously changing, and connected devices can be dynamically joined in different places (Mahmoud et al., 2015), which increases the complexity of the required security protection.

Table 1 – Summary of CPS security.

CPS layer	Components	Objective	Security issues	Security parameters	Countermeasures mechanisms
Perception layer	– RFID tag and readers – WSN – Smart Card – GPS	– Information collection	– Terminal Security – Sensor network security – Node reputation – Privacy	– Authentication – Confidentiality – Trust management	– Certification – Access control – Authentication – Data encryption – Lightweight encryption – Sensor data protection – Key agreement – Environment monitoring – Secure routing protocol – Trust management
Transmission layer	– Wireless networks – Wired networks – Computers – Components	– Information transmission	– Large number of nodes – Network routing – Networks security – Internet security – Heterogeneous technology	– Integrity – Availability – Confidentiality – Identity authentication	– Robust routing protocol – Hop by hop data encryption – Across Heterogeneous Network Authentication and key agreement – Network access control – Attack detection mechanism
Application layer	– Intelligent devices	– Information analysis – Control decision making	– Information processing – Access control problem – Information interception – Privacy – Safety	– Privacy – Authentication and key agreement – Cloud security	– End to end encryption – P2P – Intrusion detection – Trust management – User authentication and authorization

Challenges that could be faced in designing a security mechanism include prevention, detection and mitigation. Preventing the attack is a challenge due to the interaction space between cyber and physical systems (Gaddam et al., 2008). Some attackers do not only depend on direct vulnerabilities but also try to launch cross-layer attacks. Detecting attacks is the most difficult task since there is an interaction between cyber and physical space which needs detection techniques to be built for all layers of the CPS, including the application, transmission and perception layers. The major challenge is to design a security mechanism that can mitigate the effects resulting from breaching the system in the case of exceeding the prevention and detection security phases.

4.1. *Security requirements*

The security challenges in CPS can be classified into two categories: (1) the resulting challenges from heterogeneous technologies that are connected to implement the required functions; and (2) the resulting challenges from the applied security functions to achieve the necessary security. Because of its vast connectivity to the Internet, CPS security architecture will include, for example, all the security issues in the Internet, WSN and Mobile Communication Networks. CPS do not have uniform execution or computational processing capabilities to achieve high-security requirements, as in traditional IT (Zhang et al., 2011). Thus, it is very challenging to adopt any consolidated security mechanism based on a dynamically changing environment.

Most of the security proposed solutions try to address different security issues at each layer. Although such approaches might help in securing the desired part of the system, the risks might come through other parts of that system. To overcome this issue, a security architecture of CPS is used to protect security through all layers, such as information collection, transmission, and processing, from the bottom layer to the top layer (Zhang et al., 2011). Table 1 with data adopted from Bhabad and Scholar (2015), Lu et al. (2015), Suo et al. (2012), and Zhao and Ge (2013) shows most of the security requirements at each layer of the CPS as well as the security techniques that should be taken into consideration in designing any security solutions.

In the following subsections, we present a bottom-up analysis of the security requirements for each layer of the CPS since there are many security concerns at each layer that should be considered in order to protect such systems against attacks.

4.1.1. *Security analysis at the perception layer*

The primary target of this layer is object perception, identification and data collection (Jing et al., 2014). However, the number of connected devices results in additional security vulnerabilities. Attacks against such devices, with limited capabilities and usually connected through the Internet commonly using less secure wireless media, might easily achieve access to sensitive data, launch malicious programs and block access in some cases (Zhang et al., 2011). Thus, it is highly important to protect such devices and prevent any disclosure of information. Installing new devices, mostly located in external and outdoor environments, can also be one way that could be exploited by attackers to disclose information or analyze the system situation, resulting in physical attacks, such as tampering with the device components or replacing a device with another. Hence, adding any new device is another important issue that should be considered (Mahmoud et al., 2015).

Many physical layer devices lack authentication support, which in turn allows unauthorized access and discloses private information or installs malicious programs which might harm the system (Konstantinou et al., 2015). However, applying authentication to such devices is very challenging for many reasons; for example, many objects and entities with limited capabilities are involved. A suitable mechanism for achieving authentication at this layer is encryption. However, it is not applicable, in some cases, to implement sufficient cryptographic functions on constrained devices (e.g. sensors, contactless smart cards and health-care devices) due to the limitation of their resources (Katagi and Moriai, 2008). This results in the need for a lightweight authentication solution, given the limited computing capability of field devices, which is the focus of current research (Lu et al., 2014).

To summarize, authentication and access control processes would block access from invalid nodes, protecting against physical attacks; data encryption will protect data confidentiality and disclosure of private data during data transmission. The focus in the following two subsections is on the security analysis of RFID and WSN technologies as they are the most widely adopted communication technologies at the perception layer.

4.1.1.1. *RFID security analysis*. RFID is a wireless technology that remotely stores and retrieves data on devices. The main advantage of using RFID is that the target device can be identified without manual interaction. Even though RFID technology has accurate real-time features (Jing et al., 2014), many RFID tags do not include any security mechanism and the others that may provide security use hashing techniques or traditional symmetric approaches due to the constraints of power limitations, processing capabilities, and storage (Wood and Stankovic, 2010). Although RFID is broadly used and widely adopted, it poses many security issues that include uniform coding, the result of not having uniform standards which might prevent access by the reader; conflict collision, the result of transmissting data by multiple multiple RFID tags at the same time, which may cause reader disabling; privacy protection, as a result of using low-cost RFID tags, which have limited resources (e.g. weak computational capabilities and low storage); and location privacy, the result of revealing the tag position by achieving tag ID information and tracking the holder location (Jing et al., 2014).

With all the mentioned security weaknesses, RFID is still seen as a necessary part of CPS because it can achieve many operations including detecting changes in physical and environmental objects, direction of movement and velocity, temperature, humidity, gas and light sensing (Zhang et al., 2011). Regarding security issues, device authentication is an important goal and implementing a robust authentication mechanism requires tags with appropriate storage and computational capabilities. However, low-cost RFID tags do not have the required specification to implement robust security mechanisms (Jing et al., 2014). Thus, it is difficult to implement any of the widely-used security mechanisms (e.g. SSL, IPSec, PKI or Diffie–Hellman key exchange) due to the resource limitation of RFID (Premnath and Haas, 2015).

Uniform coding, conflict collision, privacy protection and location privacy are the four RFID security challenges. Thus, there is a need for a uniform encoding standard, conflict collision detecting and avoiding and lightweight data privacy protection. In RFID, integrity, authenticity and confidentiality can be accomplished using lightweight cryptographic algorithms and transmission protocol technology (Zhao and Ge, 2013) which is suitable for limited resources.

4.1.1.2. *WSN security analysis*. WSN, also called Wireless Sensor and Actuator Networks (Wu et al., 2010), are distributed sensors for monitoring the physical environment or environmental conditions, such as temperature, gas indicator and pressure. They are also defined as self-organizing networks with dynamic network topology and widely distributed multi-hop wireless networks. WSN have limited resources, such as low memory storage, computational capabilities (e.g. 8-bit or 16-bit processor architecture (Jing et al., 2014), 8 MHz clock frequency) and limited energy resources (battery) in addition to vulnerable radio conditions and minimal direct human interaction, which will be reflected in the ability to perform any security mechanism (Sheng et al., 2013).

Current research focuses on the authenticity and integrity of sensor data while disregarding confidentiality because the data can be sensed by an attacker's replaced device (Suo et al., 2012). One of security concerns related to sensor nodes is the mutual trust among sensor nodes, especially external nodes, for securing data transmission (Lu et al., 2013); in some cases, sensor nodes are deployed in an open environment and are not periodically monitored and may be susceptible to physical attacks. The main issues that are still not effectively solved when applying cryptographic algorithms are supporting a newly added node using the key pre-distribution method; storing and allocating keys; and consuming less energy by cryptographic algorithms (Jing et al., 2014).

To perform the security objectives for CPS, cryptographic algorithms, key management, secure routing and trust management can in sequence solve or eliminate the security challenges of WSN. The two types of cryptographic algorithms, asymmetric and symmetric, have been applied in WSN. However, each of these types has benefits and drawbacks. While symmetric encryption is widely adopted since it needs fewer computational calculations than asymmetric encryption, key exchange protocol has problems such as the complexity of key exchange protocol and key confidentiality (Jing et al., 2014).

The alternative method, asymmetric encryption (public key), is considered since it provides higher security with the following benefits: good scalability, proper node authentication and better security for the selected network (Suo et al., 2013). The public key cryptography will be the best option for the future, and the research will be focused on optimizing the computational processes and the used parameters (algorithm parameters).

A lightweight cryptographic algorithm that is suitable for sensor nodes has not yet been achieved (Suo et al., 2012). Ultimately, each of the asymmetric encryption and symmetric encryption approaches has features; however, overcoming all security challenges in WSN cannot be achieved by applying only one such approach (Jing et al., 2014). Hardware with optimized power consumption and optimum developed software authentication and symmetric encryption techniques can be suitable. Although asymmetric cryptography with 1024-bit keys

can be applied to ad hoc networks, it is not appropriate for WSN devices that have limited memory and computational capabilities. As an alternative, lightweight symmetric encryption techniques in addition to hashing can be applied and are the focus of most studies. Also, some enhanced asymmetric cryptographic techniques (e.g. elliptic curve cryptography (ECC)) can be afforded by devices with limited capabilities (Wood and Stankovic, 2010).

Key management, which includes generating, distributing, storing, updating and destroying the secret key, is the second important factor of WSN security. The secret key is mainly used to protect the communication channels among the nodes through the encryption process. In addition, protecting data confidentiality and integrity mostly depends on public key cryptography for which many protocols have been proposed. There have been many key distribution schemes, mainly developed by using symmetric cryptography that depends on the characteristics of sensor networks. These schemes fall into four primary key distribution protocols: simple key distribution, key pre-distribution agreement, dynamic key management, and hierarchical key management (Zhao and Ge, 2013). Thus, a need emerged for developing cryptographic key distribution approaches based on asymmetric cryptography as a network authentication protocol (Wood and Stankovic, 2010).

Applying a traditional routing mechanism in wireless networks will not be sufficient since most such protocols were mainly designed for wired networks. End-to-end authentication protocols, for example SSH and SSL, need to include certification among nodes for WSN. As a result, the focus of security in WSN was turned into using asymmetric encryption such as Elliptic Curve and NtruEncrypt (an encryption algorithm) cryptography. Trust management of nodes in WSN is mainly used for security issues of open networks. In addition to applying any authentication algorithm for sensors, it should also include trust security and privacy implementation among sensors and base stations. In this way, trust management will be involved in all network nodes and should be able to make a balance between limited resources and network security (Jing et al., 2014).

An authentication protocol that is designed specifically for WSN devices, with low storage and processing capabilities, is required. In many research studies, the focus is on only one aspect of security issues in WSN, and to strengthen their security, there should be a framework that includes the above four mentioned factors of robust cryptographic algorithms, key management, secure routing protocols, and trust management, each of which should be lightweight.

4.1.2. *Security analysis at the transmission layer*

While networks are widely used in many fields in connecting devices and bringing convenience to users, they expose various security concerns and can be easily attacked or eavesdropped on by assailants (Konstantinou et al., 2015). For instance, wireless accessibility provides users with significant convenience whereas attackers can interact with the network and cause some damage or steal valuable information (Stouffer et al., 2011). CPS communication, which introduces machine to machine communication, differs from that in the Internet, which is restricted to machine to human.

The existing network security architecture was not principally designed for machine communications (Zhao and Ge, 2013) (e.g. communication between devices in the CPS). Machine to machine data transmission poses security issues due to lack of compatibility among connected devices. These security issues cannot be solved using current network protocols that are mainly designed for use in the Internet. Although such protocols still provide some protection mechanisms, they are not the optimum solution. Attacks can employ any resulting weaknesses of heterogeneously connected devices to gain access to users' information, which can be then used for malicious activities (Mahmoud et al., 2015).

For protecting the devices in the used network, it is very important to protect the network itself. Devices should have the ability to be enabled to detect any abnormal behavior or situation that may affect the security of the system. This needs the implementation of a robust transmission protocol as well as software with Intrusion Detection at the devices' side. The security at the transmission layer can be divided into two types. The first comes from the connected devices and the second type comes from related technologies and resulting faults of the designed protocols through the implementation process. In wireless networks, the nodes are allowed to move dynamically without former authentication, resulting in more vulnerabilities that can be maliciously used to affect the security of the used network.

4.1.2.1. *Network access*. Accessing networks can be achieved using an ad hoc network or wireless networks. An ad hoc (peer-to-peer) network is a non-centric network in which communication among nodes does not need a base station (Jing et al., 2014). In this type of network, changes in the nodes can be easily adapted to a certain degree. Most security threats in this kind of network come from the radio channel, which can be eavesdropped on by attackers. The common security challenges in this network are unauthorized node access, data security and network routing security. An appropriate solution to the unauthorized node access can be achieved by enforcing authentication and authorization techniques. A suitable solution to the data security can be obtained by using authentication and encryption key management mechanisms. The solution to the routing security can be realized by implementing encryption mechanisms.

Wi-Fi network, also known as IEEE802.11, is the most widely used wireless network. It is a centric network in which the communication among nodes is accomplished through fixed bridges (base station) such as a wireless local area network. Any terminal device can wirelessly connect and communicate with applications through the Internet via Wi-Fi networks. Despite the convenience provided by Wi-Fi technology, there are many security issues, including DOS and unauthorized access attacks as well as the attacks mentioned in Section 3.2.2. To overcome such security concerns, access control and network encryption are used (Jing et al., 2014).

4.1.2.2. *Network encryption mechanisms*. There are two encryption mechanisms: hop-by-hop and end-to-end. In the hop-by-hop encryption mechanism, information is encrypted in the transmission process. This method needs to keep plaintext in each node in both the processes, encryption and decryption.

In end-to-end encryption, information can only be seen by the sender and the receiver and through all the transmission processes and forwarding nodes, data are encrypted.

If only the links among nodes need to be protected, the hop-by-hop encryption mechanism can be adopted. Although using this approach provides some features, such as high efficiency as well as low cost and latency, each node can decrypt the data. Thus, these nodes must be trusted (Suo et al., 2012). Furthermore, in this case, the security responsibility will be on the application process at the nodes. The end-to-end encryption mechanism provides many advantages, such as only the sender and receiver can read the messages and no eavesdropper can access the cryptographic keys needed to decrypt the enciphered data. However, it is very challenging to implement this method, especially when having limited end devices such as sensors. For example, SSL/TLS protocol operates end-to-end and allows setting some required security capabilities among the clients and servers (Wood and Stankovic, 2010).

Networking security is a multi-layered security system (Jing et al., 2014), and the primary network challenges in CPS come from wireless networks (Ali et al., 2015). To build a robust network security mechanism, there is a need for solid end-to-end authentication and key agreement, cross-domain authentication, cross-network authentication, and secure routing mechanisms. To prevent illegal node access and provide secure network routing, identity authentication should be considered to enhance data integrity and confidentiality.

Security architecture could be composed of two sublayers: point to point security, securing hop-by-hop transport security such as across network certification and mutual authentication; and end-to-end security, securing communications between one device/system to another. Hop transmission data could be secured by the first sublayer while data confidentiality and network availability could be secured by the second layer (Lu et al., 2013). Taking into consideration that most classical communication security techniques are not principally designed for heterogeneous applications (Wang et al., 2010), a new developed secret approach for heterogeneous applications is needed. It is important to take into consideration capacity and connectivity issues (e.g. address space) that may result in network congestion and redundancy. IP technology is not suitable for a large number of connected nodes. As a result, IPSec protocol, which provides authentication and encryption abilities, is being widely adopted (Zhao and Ge, 2013). This protocol is commonly used in establishing secure Virtual Private Networks among network peers (Wood and Stankovic, 2010). Because of constraints in using IP protocol, especially in CPS, 6LoWPAN protocol has been proposed and is used in a compression version of the IPv6 packet header. However, an aggravating overhead resulting from the residual overhead is still the main issue of this protocol (Sheng et al., 2013). Some established solutions of communication security include TLS/SSL, which can provide integrity, authenticity and confidentiality; and Internet Protocol Security (IPSec), which can provide integrity, authenticity and confidentiality in each layer (Suo et al., 2012).

4.1.3. *Security analysis at the application layer*

This layer includes many applications, each of which has its own vulnerability that can affect CPS security. In addition, gaining user privacy protection and sensory data hierarchical access are the prime challenges for the application layer (Wang et al., 2010). This layer may contain different applications such as services and industrial monitoring as in Smart Homes and Smart Cities. The main security concern is the vulnerabilities that might result from the design which can be exploited by adversaries to attack the system. Thus, malicious code or software can be launched to affect system security. Another security concern can be a result of integrating various techniques, which might impede data processing, resulting in a bottleneck in the system. These security issues can affect the availability and reliability of the system (Bhabad and Scholar, 2015). Some references, such as Atzori et al. (2012), mention trust as a part of security. However, security does not require the existence of trust, and incorporating trust in the system is a complex process and produces overheads.

Security at the application layer includes information accessing, user authentication, information privacy and collapsing used data links, platform stability and management (Jing et al., 2014). Moreover, each application has its security requirements, and there is an increased demand for providing such requirements since the application of important and sensitive systems, which are being monitored and controlled in real-time, is growing (Wood and Stankovic, 2010). In fact, the number of complex security issues that needs to be considered depends on the type of application (Zhao and Ge, 2013). Hence, it is difficult to design applications which are fully trusted among themselves without taking into account the underlying executed operations of the system, such as connectivity and data generated by CPS (Trappe et al., 2015). Another issue is that different industry standards have different CPS applications. Currently, no global standard governs the interaction and development of applications of the CPS application layer, which enhances the lack of security (Krco et al., 2014; Mahmoud et al., 2015). This means that different security needs are required for different application environments (Zhao and Ge, 2013).

When designing CPS applications, there are many security issues that should be considered, including: different authentication mechanisms for various applications, which make integration very complex when guaranteeing identity authentication; a large number of connected devices and shared data that result in large application overhead, which will be reflected in the availability of the provided services by such devices; the large number of users who interact with the applications; the amount of data revealed and more responsibility for application management (Mahmoud et al., 2015).

5. CPS security solutions

The importance and requirement of security are different from one application to another. For example, in Intelligent Transportation and Intelligent Medical, data privacy is most important requirement whereas in Intelligent Urban Management and the Smart Grid, data authenticity is more important. There have been many efforts to produce a secure CPS model. Some security solutions and modeling techniques to address security in CPS are presented in this section. The following two subsections present CPS security solutions based on the considered

layers in the proposed solution. Section 5.1 lists the individually provided solutions per layer, and Section 5.2 lists proposed solutions as frameworks that consider different solutions at each layer.

5.1. *Single-layer solutions*

Regarding key management for encryption techniques, in Yang et al. (2006) an improved identity-based key distribution scheme for WSN using ECC key management is proposed. A study of using small cryptographic keys in asymmetric encryption for WSN is presented in Premnath and Haas (2015). This study shows that, to a great extent, there is a decrease in the computational processes by using smaller key sizes among nodes. It also provides a key breaking cost estimation in a situation of limited available resources (cost in dollar and time in a number of days), and a trade-off between the required time of privacy protection against the processing load for a node. The results show that using a small 1024-bit public key modulus requires a node to perform only 3.1% of the computations relative to a typical 3248-bit modulus. This study also provides an estimation of the required number of days that are needed by an adversary to break different small-sized keys used in the communication between the node and household Smart Meters and utility company servers.

A lightweight authentication protocol is proposed in Trappe et al. (2015) for securing RFID tags to prevent attackers from gaining access to the network by sniffing the Electronic Product Key of the victim tag and programming it to another tag. Also, to prevent attacks, this protocol can ensure mutual authentication among RFID readers and tagged items with low overhead on devices. In Wang et al. (2011), the authors propose cyber-physical enhanced secured WSN that integrate cloud computing for u-life care architecture as well as healthcare application. Monitoring and decision making are also provided in the same system. This architecture combines three fundamental parts: communication, computation and resource scheduling and management. The security core is a combination of a source sensor node with an encrypted random number for providing protection against attacks. The focus of the security core is on enhancing WSN and integrating them into cloud computing. This research provides analysis and explanation for the proposed models such as real-time scheduling, security models and cloud computing.

To enhance security for a Smart Grid, which fundamentally depends on three critical security requirements (authentication, authorization and message integrity) a lightweight two-step mutual authentication scheme for distributed Smart Meters at different hierarchical networks is proposed in Fouda et al. (2012). Shared key session exchange is achieved using Diffie–Hellman exchange protocol, and the messages among Smart Meters are authenticated using the shared session key and hash-based authentication code technique.

From the perspective that there is a need for a multi-factor authentication for CPS devices, a new hardware-based security technique for CPS is presented in Kirkpatrick et al. (2009), which is specifically for devices with limited computing power. This method uses the Physically Unclonable Function (PUF), also called the Physical Random Function, for device access restriction with assigned keys. PUF is a function that provides a unique value depending on the physical properties of the hardware of the used device. This mechanism is used as a unique identifier to certain devices as a zero-knowledge identity proof. This approach depends on the fact that the physical limitations of manufacturing devices introduce minor differences among any copies of the same hardware, which gives each device a unique identity that can be identified by the PUF value.

PUF is implemented in the hardware, such as using SRAM, to unambiguously identify the devices. In addition, this technique can be utilized for location base access control and encryption. The advantage of using PUF is that it produces a unique value, which, for each hardware instance, is the same as repeating the PUF implementation on the same device. Thus, the PUF can be used to confirm the unique identity of CPS devices, ensuring the integrity and authenticity of the connected device. PUF can also be used for creating unique cryptographic keys. The common usage of this technology is in securing the storage of cryptographic keys. Since they will be bound to the hardware, it would be difficult for an adversary to obtain these keys.

Another approach for enhancing security is by including IDS techniques. Considered one of the technologies for discovering adversaries in the transmission layer, this can timely monitor node behavior to identify any suspicious behaviors (Zhao and Ge, 2013). As mentioned in Section 3.3.2, IDS is out of the scope of this paper, but the reference Mitchell and Chen (2014) presents a comprehensive literature review regarding research directions in CPS IDS techniques, and summarizes the most studied techniques in the field.

5.2. *Multi-layer solutions*

Dealing with a single measure, such as the listed solutions in the previous subsection, might not be enough in solving the security issues, which should be considered from a multi-measure perspective. Moreover, fulfilling security in one layer will not satisfy the required security objectives, such as implementing a robust security solution at the sensor level of a system with a weak application layer. Therefore, there should be cooperation among the three layers of the system and cross-domain security solutions. As the security for CPS will not be entirely accomplished by individually implementing a single solution in each layer, some researchers focus on developing security solutions as a framework for all CPS layers together. However, each layer has different requirements which, in turn, lead to the increased complexity of any produced solution. Thus, the focus must be on developing an alternative mechanism to fit limitations in used devices.

An off-line authentication mechanism that relies on a Combined Public Key (CPK) is presented in Zhang et al. (2011). The main objective of this mechanism is to solve the security issues that are related to cross-domain authentication with massive data sets of authentications. The proposed security architecture provides security preservation for sensor data, tag privacy and data transmission. The applied approach includes authentication validity of the integrating nodes as well as identification distinction. In order to improve cyber security, the three layers (application, transmission and perception) are taken into consideration for constructing the trusted system. At the application

layer, trusted access control is used to enhance legal access, uniquely validate the connected devices and ensure the process of non-repudiation. Then, code authentication trusted thread and process are performed to save the runtime in open and unsafe network environments. After that, a trusted database is used to provide data access mutual authentication. The proposed authentication mechanism eliminates the need of relying on third party certification. At the transmission layer, a CPK special communication chip is embedded with wireless-oriented or wired communication equipment; thus, avoiding the need for certification from a third party. At the perception layer, tags are embedded with Elliptic Curve Cryptographic (ECC) algorithms to provide authorized access, and used with the CPK, which is identity-based authentication, to provide fast authentication.

A security analysis of the CPS is presented in Neuman (2009), which provides some of the characteristics, such as distributed management and control, feedback, real-time requirements, and geographic distribution, that should be considered in designing security solutions. The focus of this study is on the physical control of the CPS, with given suggestions for protecting communication channels, real-time requirements, and applications. A security framework for CPS, as proposed in Lu et al. (2014), provides a comprehensive analysis regarding three aspects of security objectives, security in specific CPS applications, and security approaches. However, this study does not consider authenticity in CPS security objectives, which is a major factor.

Vegh and Miclea propose a method of designing a secure cyber-physical system model (Vegh and Miclea, 2014) by combining both cryptography and steganography. The authors propose a modeling security framework through hierarchical access to information to increase the security level. This method involves encrypting and hiding data, and hiding the secret key in a different cover file. It is considered that the pattern of combining security algorithms in the same system will enhance required data protection in CPS. This system is built on a multi-agent idea, and each agent has incomplete decentralized data to solve the tasks. This implies that each agent (user) has a local view of the system and has no chance to view the entire information of that system. For example, tree root has full access to the information inside the system, while the rest have limited access. Hierarchical access to information gives some access restriction to information. The ElGamal algorithm, as used in the proposed system for securing CPS, has three main stages: key generation, encryption, and decryption.

Trust, the probability of performing the required actions by objects, is not considered by many researchers. Ali et al. (2015) proposes a trust-based approach with two-tier blankets, which consist of internal and external trust layers, to create a reliable and secure CPS. For ensuring secure and reliable communications in CPS, the authors take into consideration the following points: users' authentication prior to joining the network; a trust relationship between different nodes of the CPS; joining malicious nodes that may attack the key nodes of the CPS (sensors or actuators); and reconfiguring the CPS system in a situation of aggression. The idea of the proposed approach is to involve security as an integral part of CPS architecture rather than applying it as a complementary solution. In addition to CPS security objectives, the authors consider a trust-oriented approach as a fifth objective that will enhance the security target.

Taking into consideration that devices can physically move from one holder to another, Xie and Wang (2014) discuss the importance of trust among users with proper permissions and access control. This work presents a mutual trust idea for inter-system security, which can be implemented by creating an item-level access-control framework. This trust is based on key creation and a token that is created by the owner or the manufacturer of the RFID and assigned to the device. When assigning this device to a new user, permission can be changed by the owner or the device itself. Thus, the permission of the device can be substituted between the previous user and the new user, without extra overhead. This process aims to reduce the overhead of assigning keys, which are generated by the manufacturer of the RFID device, by an entitlement system. A CPS security framework is presented in Lu et al. (2013) based on three layer architecture: interpretation (perception), transmission (network), and cyber (application). Multiple security mechanisms are set in the information (cyber) field using a hierarchical network structure to increase security levels, whereas control domain security is treated by, for instance, using distributed estimation or tolerant control. This method primarily provides a security framework for CPS, depending on potential threat analysis. A risk assessment operation is taken into consideration from the perspective of assets (values), threats, vulnerabilities and damage.

Wang et al. (2010) propose a context-aware security framework for general CPS, which is a set of environmental situations and settings to determine the behavior of a user or an application's event. The proposed security framework comprises three essential security parts: sensing, cyber and control. This framework uses parameters to determine the behavior of the system, situational information and environmental situations to calculate the level of security of the system and to improve information security decisions. It makes relevant context information that is integrated into multi-security measures, for example, encryption, key agreement and access control, to make an adapted CPS security for the physical environment. The main objectives of the proposed context-aware security framework are confidentiality, availability, integrity and authenticity. This method categorizes the function of CPS into the following four stages: monitoring physical processes and the environment; networking, which includes data aggregation and diffusion; computing to collect and analyze data during the monitoring phase; and an actuating stage to execute the determined action in the computation stage. The aim of this method is to make a security mechanism for CPS that dynamically adapts to the physical environment.

6. Discussion and future research areas

As listed in Section 3.2, each layer of the CPS faces the threat of many attacks. Handling each attack singly will not help, but will burden or exhaust system resources. Much work has been accomplished in the field of CPS security; however, applying common classical methods, such as cryptography and steganography, to CPS is not sufficient. Furthermore, such methods were not principally designed for interaction operations for dif-

ferent applications. Any CPS security model should include security defense layers with the following characteristics: difficult penetration; robust authentication and access control mechanism; high response time; upgrade capability and attack mitigation abilities. Such system can be implemented using a hybrid model by integrating a robust hierarchical access model and context-aware security framework involving a lightweight cryptographic technique as well as adopting an immune security assessment model. The assessment model should consider that vulnerabilities and threats are not static, and that their attacks and behaviors periodically change.

Another important factor is that attacks might not only come from outside of the system but also from inside, such as from employees who do not need much additional knowledge about the target system. The knowledge that insiders possess often gives them unrestricted access to steal or modify data in the system or to deactivate that system. Hierarchical access to information, such as presented in Vegh and Miclea (2014), would improve security. Although the ElGamal algorithm has been used in the presented solution, the key generation stage is a complicated process. While the proposed mechanism provides restricted access for users, it is not suitable for CPS, mainly because of the dynamic changes of the used devices. Enforcing the access rights of users to the system will increase the overall security and decrease insider attacks. However, hierarchical access to information is difficult to implement because this increases the overhead and causes difficulty for devices with limited resources in performing complex operations. The better option is to adopt a robust access control model, which is enhanced with contextual information that ensures authenticity and confidentiality as well as increases the overall security of CPS.

To protect the CPS network from joining malicious nodes at the perception layer (physical attack), a robust authentication process is required. PUFs can be used to confirm the unique identity of CPS devices, which ensures the integrity and authenticity of connected devices, and can also be used for creating unique cryptographic keys. However, the main limitation of this approach is that many hardware devices are not provided with PUF implementation ability, such as RAM. In addition, not all devices can implement PUF technology. Thus this technique cannot be widely adopted.

A more efficient approach for dealing with security in CPS is by using a multi-layered approach where the security of the system is considered at the beginning of the design for each layer. There must also be a correlation between the security that will be implemented with cost and time. Furthermore, the three-layer architecture of CPS is suitable for realizing the technical issues at the beginning stages of security analysis. Another issue should be considered as one of the challenges for CPS is the heterogeneous data that collected from different devices, each of which uses different protocols leading to compatibility issues related to data format and communication protocols. The main challenge in CPS is designing protocols that can work on different devices and situations. Thus, there is a need for a unified encoding standard for information exchange protocols for each device, such as RFID and WSN, which have different information access formats, security control mechanisms and storage formats, all of which lead to different data processing approaches. A unified data processing standard will help in reducing transmission costs by using data compression and data fusion techniques. Furthermore, cloud computing can supply the required data storage with affordable cost and performance. These advantages can be exploited by CPS in connecting a large number of devices with limited capabilities. In this case, the computation processes can be efficiently accomplished at the cloud computing layer.

The prominent cryptographic encryption technique is the Identity-Based which uses short encryption keys and is considered stronger than other cryptographic techniques in terms of computation, efficiency and certification (certificate less). Another important security issue that is still not completely solved when applying security solutions is that of supporting newly added nodes. This can be overcome by enhancing any used security technique with contextual information.

7. Summary

Since it is a comparatively new area, limited work has been accomplished in the security field of CPS. Prior to developing any security model, there is a real need for appropriate analysis and anticipation ability for adversaries. Additionally, the verification process of any proposed security model must not affect real-time operations in the system. Therefore, performing assessment, authentication and access control processes should take place without disrupting the runtime environment. This way helps to identify mitigating options after inferring risk assessment. The transmission media of CPS may include different sensors, data types, real-time generated data, process analysis and various application interactions. Thus, it is necessary to ensure that the system is secure while interacting with other systems. Enhancing CPS security using security mechanisms such as encryption algorithms, authentication protocols and steganography will not address all security risks that might be faced. Such solutions might help to protect the targeted systems to some point. However, any solution should consider the application situation and context as part of assessing security risks. Thus, enhancing the application security will improve the security of the whole system.

A security mechanism should be designed for the entire system rather than in a single layer. This involves developing an integrated cross-layer security solution that deals with various security architectures and securely integrates data from different sources. It is difficult to produce a CPS security architecture that handles all potential attacks in a single model. Therefore, there is a need to develop a protocol that handles security mechanisms on the three layers of the CPS. The best possible solution could be the PUF that can provide a unique identity for CPS devices. On the other hand, many hardware devices are not provided with PUF implementation ability, hence not all devices can implement PUF technology. Therefore, at this time, this technique cannot be widely adopted. According to the CPS attacks mentioned in Section 3.2, it can be concluded that the most common security targets are sensors and actuators at the perception level; data leakage, DoS, control or destruction at the transmission level; and privacy disclosure and unauthorized access at the application level.

Privacy is another important issue that should be considered and preserved in any provided solution. Protecting users'

privacy from eavesdropping or theft can be accomplished by a context-aware privacy protection and encryption scheme, while preventing man-in-the-middle attacks and authenticity can be achieved by using context-aware mutual authentication protocol. Use of context-aware access control can prevent unauthorized access. Preventing key leakage and providing a key management mechanism can be achieved by using context-aware key management. Finally, detecting and blocking intrusions can be achieved by using context-aware intrusion detection. There is a real need to develop alternative methods in addition to a security requirement-based risk assessment approach without relying on traditional assessment methods. A robust evaluation model for verifying all threats and vulnerabilities is still an open research. The system will rely on context-based authentication and access control mechanisms for insider attacks, cryptographic algorithms for confidentiality, and a robust assessment model for anticipation attacks and mitigation processes.

Although all the security objectives of the CPS are important, authenticity, validating claimed identity, should be ranked as the first objective of the security on which the other security classes are built. Without ensuring that the authorized party is who it claims to be, other security objectives would be useless. In addition, any cryptographic technique used to satisfy security objectives should be lightweight in order to be affordable for devices with limited capabilities. This, in turn, helps to overcome the constraints of such devices. Ultimately, authentication is the most effective and important approach in addressing many security risks. A robust authentication mechanism will prevent unauthorized entities from joining the CPS environment and causing security issues. Even though many authentication techniques have been developed, there is still a need for robust and usable authentication techniques that enhance decision making by involving contextual information. The prominent cryptographic encryption technique is the Identity-Based which uses short encryption keys and is considered stronger than other cryptographic techniques in terms of computation and efficiency.

REFERENCES

Ali S, Anwar RW, Hussain OK. Cyber security for cyber physical systems: a trust-based approach. J Theor Appl Inf Technol 2015;71(2):144–52.

Alvaro C, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S. Challenges for securing cyber physical systems. Work Futur Dir Cyber-Phys Syst Secur 2009;5.

Asare P, Broman D, Lee EA, Torngren M, Sunder SS. Cyber-physical systems [Online]; 2012. Available from: http://cyberphysicalsystems.org/. [Accessed 24 December 2016].

Ashok A, Hahn A, Govindarasu M. A cyber-physical security testbed for smart grid: system architecture and studies, Proc. Seventh Annu. Work. Cyber Secur. Inf. Intell. Res. ACM, 2011.

Atzori L, Iera A, Morabito G, Nitti M. The Social Internet of Things (SIoT) – when social networks meet the internet of things: concept, architecture and network characterization. Comput Netw 2012;56(16):3594–608.

Bhabad MA, Scholar PG. Internet of things: architecture, security issues and countermeasures. Int J Comput Appl 2015;125(14).

Bhattacharya R. A comparative study of physical attacks on wireless sensor networks. Int J Res Eng Technol 2013;72–4.

Cárdenas A., Amin S., Lin Z.-S., Huang Y., Huang C.-Y., Sastry S., Attacks against process control systems: risk assessment, detection, and response, Proc. 6th ACM Symp. Information, Comput. Commun. Secur. ACM, pp. 355–366, 2011.

Chang E, Machizaud M, Dunn M. Advances in Internet of Things and cyber physical systems and its adoption to smart ship, Int. Conf. Wirel. Commun. Network, Balt. USA, 2015.

Chen G. Internet of Things towards ubiquitous and mobile computing, Microsoft Res. Asia Fac. Summit, Shanghai, 2010.

Fouda MM, Fadlullah ZM, Kato N, Lu R, Shen XS. A lightweight message authentication scheme for smart grid communications. IEEE Trans Smart Grid 2012;2(4):675–85.

Gaddam N, Kumar GSA, Somani AK. Securing physical processes against cyber attacks in cyber-physical systems, Natl. Work. Res. High-Confidence Transp. Cyber-Physical Syst. Automotive, Aviat. Rail, Washingt. DC, pp. 2–4, 2008.

Gamundani AM. An impact review on Internet of Things attacks, Int. Conf. Emerg. Trends Networks Comput. Commun., pp. 114–118, 2015.

Gładysz B. An assessment of RFID applications in manufacturing companies. Manag Prod Eng Rev 2015;6(4):33–42.

Gou Q, Yan L, Liu Y, Li Y. Construction and strategies in IoT security system, Proc. - IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom., pp. 1129–1132, 2013.

Hu W, Oberg J, Barrientos J, Mu D, Kastner R. Expanding gate level information flow tracking for multilevel security. IEEE Embed Syst Lett 2013;5(2):25–8.

Jalali S. Trends and implications in embedded systems development, Tata Consult. Serv. Limited, TCS white Pap., 2009.

Jing Q, Vasilakos AV, Wan J. Security of the internet of things: perspectives and challenges. Wirel Netw 2014;20(8): 2481–501.

Kao J, Marculescu R. Eavesdropping minimization via transmission power control in ad-hoc wireless networks. Sens Ad Hoc Commun Netw 2006;2:707–14.

Katagi M, Moriai S. Lightweight cryptography for the Internet of Things, Sony Corp., pp. 7–10, 2008.

Khan R, Khan SU, Zaheer R, Khan S. FUTURE Internet: the Internet of Things architecture, possible applications and key challenges, 10th Int. Conf. Front. Inf. Technol., pp. 257–260, 2012.

Kirkpatrick M, Bertino E, Sheldon FT. Restricted authentication and encryption for cyber-physical systems, DHS CPS Work. Restricted Authentication Encryption Cyber-physical Syst., 2009.

Konstantinou C, Maniatakos M, Saqib F, Hu S, Plusquellic J, Jin Y. Cyber-physical systems: a security perspective, 20th IEEE Eur. Test Symp., pp. 1–8, 2015.

Krco S, Pokric B, Carrez F. Designing IoT architecture(s): a European perspective, IEEE World Forum Internet Things, WF-IoT, pp. 79–84, 2014.

Kumar JS, Patel DR. A survey on internet of things: security and privacy issues. Int J Comput Appl 2014;90(11):20–6.

La HJ, Kim SD. A service-based approach to designing cyber physical systems, IEEE/ACIS 9th Int. Conf. Comput. Inf. Sci., pp. 895–900, 2010.

Leavitt N. Researchers fight to keep implanted medical devices safe from hackers. Computer 2010;43(8):11–14.

Li Y, Shi L, Cheng P, Chen J, Quevedo DE. Jamming attack on cyber-physical systems: a game-theoretic approach, Cyber Technol. Autom. Control Intell. Syst. (CYBER), IEEE 3rd Annu. Int. Conf., pp. 252–257, 2013.

Lu T, Xu B, Guo X, Zhao L, Xie F. A new multilevel framework for cyber-physical system security, pp. 2–3, 2013.

Lu T, Lin J, Zhao L, Li Y, Peng Y. An analysis of cyber physical system security theories, 7th Int. Conf. IEEE, pp. 19–21, 2014.
Lu T, Lin J, Zhao L, Li Y, Peng Y. A security architecture in cyber-physical systems: security theories, analysis, simulation and application fields. Int J Secur Appl 2015;9(7):1–16.
Maheshwari P. Security issues of cyber physical system: a review. Int J Comput Appl 2016;7–11.
Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of Things (IoT) security: current status, challenges and prospective measures, 10th Int. Conf. Internet Technol. Secur. Trans. IEEE, pp. 336–341, 2015.
Miclea L, Sanislav T. About dependability in cyber-physical systems, Proc. IEEE East-West Des. Test Symp. EWDTS, pp. 17–21, 2011.
Mitchell R, Chen I. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv 2014;46(4):1–29.
Mo Y, Sinopoli B. Integrity attacks on cyber-physical systems, Proc. 1st Int. Conf. High Confid. Networked Syst., pp. 47–54, 2012.
Moteff J. Risk management and critical infrastructure protection: assessing, integrating, and managing threats, vulnerabilities and consequences, Libr. Congr. Washingt. DC Congr. Res. Serv., pp. 1–28, 2005.
Neuman C. Challenges in security for cyber-physical systems. DHS ST Work Futur Dir Cyber-Phys Syst Secur 2009;7:1–4.
NIST, Cyber-physical systems: situation analysis of current trends, technologies, and challenges, Natl. Inst. Stand. Technol (NIST), Columbia, Maryland, 2012.
Nourian A, Madnick S. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. IEEE Syst J 2015. doi:10.1109/TDSC.2015.2509994.
Peng Y, Lu T, Liu J, Gao Y, Guo X, Xie F. Cyber-physical system risk assessment, Ninth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process., pp. 442–447, 2013.
Premnath SN, Haas ZJ. Security and privacy in the internet-of-things under time-and-budget-limited adversary model. IEEE Wirel CommunLett 2015;4(3):277–80.
Raza S. Lightweight security solutions for the Internet of Things, Mälardalen University Press Dissertations, Mälardalen University, Västerås, Sweden, 2013.
Sendler U. Industrie 4.0 – Beherrschung der Industriellen Komplexität mit SysLM (Systems Lifecycle Management), Ind. 4.0, Springer Berlin Heidelb., pp. 1–19, 2013.
Shafi Q. Cyber physical systems security: a brief survey, Comput. Sci. Its Appl. (ICCSA), 12th Int. Conf. IEEE, pp. 146–150, 2012.
Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, Leung KK. A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wirel Commun 2013;(6):91–8.
Shipley AJ. Security in the Internet of Things, lessons from the past for the connected future, Secur. Solut. Wind River, White Pap., 2013.
Soldatos J. IoT vs. M2M, CPS, WoT: Are these terms synonyms?, [Online]; 2015. Available from: https://www.linkedin.com/pulse/iot-vs-m2m-cps-wot-terms-synonyms-john-soldatos. [Accessed 24 December 2016].
Stankovic JA. Research directions for the internet of things. IEEE Internet Things J 2014;3–9. no. c.
Stouffer K, Falco J, Scarfone K. Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology, NIST Spec. Publ. 800-82, 2011.
Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. Int Conf Comput Sci Electron Eng IEEE 2012;3:648–51.
Suo H, Liu Z, Wan J, Zhou K. Security and privacy in mobile cloud computing, 9th Int. Wirel. Commun. Mob. Comput. Conf. (IWCMC), IEEE, pp. 655–659, 2013.
Trappe W, Howard R, Moore RS. Low-energy security: limits and opportunities in the internet of things. IEEE Secur Priv2015;13(1):14–21.
Vegh L, Miclea L. Enhancing security in cyber-physical systems through cryptographic and steganographic techniques, Autom. Qual. Testing, Robot. Int. Conf. IEEE, pp. 1–6, 2014.
Vermesan O, Roy B. Internet of Things and cyber-physical systems – SINTEF, [Online]; 2016. Available from: http://www.sintef.no/en/information-and-communication-technology-ict/communication-systems/internet-of-things-and-cyber-physical-systems/. [Accessed 26 December 2016].
Wang EK, Ye Y, Xu X, Yiu SM, Hui LCK, Chow KP. Security issues and challenges for cyber physical system, Proc. IEEE/ACM Int'l Conf. Green Comput. Commun. Int'l Conf. Cyber, Phys. Soc. Comput., pp. 733–738, 2010.
Wang J, Abid H, Lee S, Shu L, Xia F. A secured health care application architecture for cyber-physical systems. Control Eng Appl Inform 2011;101–8.
Weiss J. Control system cyber vulnerabilities and potential mitigation of risk for utilities, White Pap. Juniper Networks, Inc., 2010.
Wood AD, Stankovic JA. Security of distributed, ubiquitous, and embedded computing platforms, Wiley Handb. Sci. Technol. Homel. Secur., pp. 1–14, 2010.
Wu M, Lu T, Ling F, Du H. Research on the architecture of Internet of Things, Proc. 3rd Int. Conf. Adv. Comput. Theory Eng., pp. 20–22, 2010.
Xie Y, Wang D. An item-level access control framework for inter-system security in the internet of things. Appl Mech Mater 2014;548:1430–2.
Yang G, Rong CM, Veigner C, Wang JT, Cheng HB. Identity-based key agreement and encryption for wireless sensor networks. J China Univ Posts Telecommun 2006;6:54–60.
Zalewski J, Drager S, McKeever W, Kornecki AJ. Threat modeling for security assessment in cyberphysical systems, Proc. Eighth Annu. Cyber Secur. Inf. Intell. Res. Work. - CSIIRW '13, p. 1, 2013.
Zhang B, Ma X, Qin Z. Security architecture on the trusting internet of things. J Electron Sci Technol 2011;9(4):364–7.
Zhao K, Ge L. A survey on the Internet of Things security, Ninth Int. Conf. Comput. Intell. Secur., pp. 663–667, 2013.

Yosef Ashibani is a PhD student in the Department of Electrical, Computer and Software Engineering at the University of Ontario Institute of Technology. His research interests include cyber-physical systems (CPS), Internet of Things (IoT) and smart home security.

Qusay H. Mahmoud is a Professor of Software Engineering in the Department of Electrical, Computer and Software Engineering at the University of Ontario Institute of Technology in Canada. He was the Founding Chair of the Department and served as Chair between Jan 2013 and June 2015, and more recently he has served as Associate Dean of the Faculty of Engineering and Applied Science at the same university. His research interests include distributed systems and software security.