A Survey on Security Issues of M2M Communications in Cyber-Physical Systems

Dong Chen[1] and Guiran Chang[2]
[1]School of Information Science and Engineering, Northeastern University
Shenyang, China
[e-mail: chend.2008@gmail.com]
[2]Computing Center, Northeastern University
Shenyang, China
[e-mail: chang@neu.edu.cn]
*Corresponding author: Dong Chen

August 31, 2011; revised December 16, 2011; accepted January 12, 2012; published January 31, 2012

Abstract

In this paper, we present a survey of security and privacy preserving issues in M2M communications in Cyber-Physical Systems. First, we discuss the security challenges in M2M communications in wireless networks of Cyber-Physical Systems and outline the constraints, attack issues, and a set of challenges that need to be addressed for building secure Cyber-Physical Systems. Then, a secure architecture suitable for Cyber-Physical Systems is proposed to cope with these security issues. Eventually, the corresponding countermeasures to the security issues are discussed from four aspects: access control, intrusion detection, authentication and privacy preserving, respectively. Along the way we highlight the advantages and disadvantages of various existing security schemes and further compare and evaluate these schemes from each of these four aspects. We also point out the open research issues in each subarea and conclude with possible future research directions on security in Cyber-Physical Systems. It is believed that once these challenges are surmounted, applications with intrinsic security considerations will become immediately realizable.

Keywords: M2M, security, privacy preserving, cyber-physical systems

This work is supported by the National Natural Science Foundation of China under Grant No. 60903159 and the Fundamental Research Funds for the Central Universities under Grant No. N100604012.

DOI: 10.3837/tiis.2012.01.002

1. Introduction

Cyber-physical systems will have to support various communication technologies and integrate different devices. A Cyber-Physical System (CPS) aims at monitoring the behavior of physical processes and actuating actions to change their behaviour in order to make the physical environment work correctly [1][2]. Usually, a typical CPS consists of two major components, physical processes and an intelligent cyber system. Physical processes are usually monitored and controlled by the cyber system which is often a networked system of several tiny smart devices with sensing, computing and wireless communication capabilities. The emergence of CPS applications have effect on the revolution including assisted living, intelligent traffic control and safety, energy conservation, enviromental control, instrumentation and avionics. However, as the interaction between the physical and cyber world increases, the physical systems become increasingly more susceptible to the security vulnerabilities in the CPS. The security and privacy preserving issues must be addressed before CPS could be widely deployed.

M2M (Machine to Machine) covers various technologies, including sensing, communications, computing, data processing and feedback control technologies, and support massive heterogeneous smart devices to communicate with each other. Nowadays, M2M has become an indispensable component for next generation networks, e.g. CPS and Internet of Things (IoT). M2M has been widely applied to a lot of novel intelligent applications and services, and may even lead to M2H (Machine to Human) and M2S (Machine to System) in the future. So far, M2M communication has been considered as one of the next frontiers in wireless network of CPS and IoT. However, it is not practically feasible to enforce the global communication security of wireless network, since massive M2M smart terminals are expected to be deployed in a highly heterogeneous distributed CPS network. M2M communication is a novel frontier in CPS systems. The research on M2M communication security issues in CPS systems is still rare. Although there are many related works on security issues in WSN (Wireless Sensor Networks), Ad-hoc networks, MANETs (Mobile Ad-hoc Networks) and etc., they cannot be applied to CPS applications directly. [3] presents a survey on security issues in WSNs, and highlights the advantages and disadvantages of various WSN security protocols. [4] proposes a survey on security issues in mobile ad hoc and sensor networks. [5] investigates the security challenges and issues in CPS systems, and proposes a context-aware security framework for general CPS systems.[6][7][8][9][10][11][12] and [13] have discussed some security issues that may occur in CPS systems. Just like other new fields, most of the research work seems to be focused on those mapping solutions from existing domains, such as WSN, which share the networked operation and low capability characteristics with CPS. However, conventional secure M2M communication solutions are not appropriate for the interoperation among novel heterogeneous applications. How to make sure that M2M communication in a system is still secure while interacting with another one is an important issue in CPS. There are also other new security issues in CPS that needs to be addressed.

The remainder of the paper is organized as follows. In Section 2, the novel security and privacy challenges are presented in details for CPS systems. Then in Section 3, a secure architecture is proposed and the security challenges of CPS systems are further discussed in details. Security issues and corresponding countermeasures are introduced and analyzed in Section 4 from four aspects: access control, intrusion detection, authentication and privacy

preserving, respectively. Open research issues in each subarea are also pointed out in Section 4. Section 5 concludes with possible future research directions on security in CPS systems, followed by the conclusion and future work of the paper in Section 6.

2. Security Issues in M2M communications in CPS

In this section, the differences between CPS and other wireless networks are pointed out firstly in order to analyze the security and privacy preserving challenges involved in M2M communications of CPS systems. Then the security challenges are analyzed, since the existence of tiny computing devices which form ubiquity in CPS domain makes the wireless networks of CPS very vulnerable to different security attacks.

A typical CPS system usually consists of several tiny devices connected together to form a collaborative computing environment. However, CPS systems commonly impose peculiar constraints in terms of connectivity, computational power and energy budget, which make it significantly different from those existing distributed systems. In order to circumvent the security problem in M2M communications in CPS systems, networks and devices need to be secured.

There are significantly different key properties between CPS and other existing network systems which cause security issues and raise novel security requirements. Many CPS applications have mission-critical tasks and thus require that security and privacy must be considered during the design period. Improper use of data and contextual information may cause serious information leakage and provide inaccurate feedback controls. While some aspects of CPS are similar to traditional wireless network based systems, such as WSN**s**, Ad-hoc Network, MANETs and so on, significant distinctions exist which greatly affect how security is achieved and guaranteed. The differences between CPS and other wireless network infrastructures are as follows. First, the device population of CPS systems is growing rapidly. It means that massive everyday things are increasingly integrated into the global CPS network. With the help of 6LoWPAN and IPv6 communication protocols, more and more sensors, sensor-embedded things, 3G phones, PDA and other smart devices are connected to IoT/NGI (Next Generation Internet) through different access technologies. Note that CPS employs IoT/NGI as the backbone network in order to realize the exchange and feedback control between cyber world and physical world. Therefore, it is so difficult for us to monitor privacy concerns. Second, sensors/actuators are usually heterogeneous and limited in computation, memory and power resources. Heterogeneous smart devices may span a range of computational abilities from PCs to RFID tags. Therefore, trust and privacy management mechanisms must accommodate even the simplest devices. Exhausted nodes may cause the route failure and dynamic adjustment of the underlying topology of the whole wireless network. Third, the topology of the underlying wireless networks change very frequently due to the failures or mobility of the smart nodes. Last but not the least, CPS applications may employ several heterogenous networks as its edge access networks to IoT/NGI in order to get intelligent services from different fields. Most networks of CPS systems are wireless networks through which sensors, sensor embedded devices, 3G phones and other smart devices can connect to IoT/NGI ubiquitously. A wide range wireless links can be employed, such as Bluetooth, Wi-Fi, ZigBee, 802.11, WiMAX, GSM, WCDMA and etc.

These differences greatly affect how secure data-transfer schemes are implemented in CPS. The research on security issues in CPS is to protect the data and contextual information from attacks and misbehaviors. As shown in **Fig. 1**, the security requirements of M2M communications in CPS systems mainly include, (1) Availability, which ensures that CPS

services are available even in the presence of Denial-of-Services (DOS) attacks. (2) Integrity, which ensures that the messages transmitted in the network are not modified by adversaries or malicious intermediate nodes. (3) Authorization, which ensures that only those authorized entities can access the service providing nodes. (4) Authentication, which ensures that M2M communication channels between two nodes are secure and malicious nodes are not involved in the communications. (5) Confidentiality, which ensures that a specific message can only be understood by the desired recipients. (6) Freshness secrecy, a node should not be able to read any previously transmitted messages when it joins the network and any future messages after it leaves the wireless network. Recently there have been heightened security and privacy concerns over various wireless networks with the emergence of CPS and IoT. However, due to the constraints of M2M communications in CPS, existing schemes, policies and mechanisms are thus inadequate and thus novel models and mechanisms are needed to protect the M2M communications in such novel CPS applications.

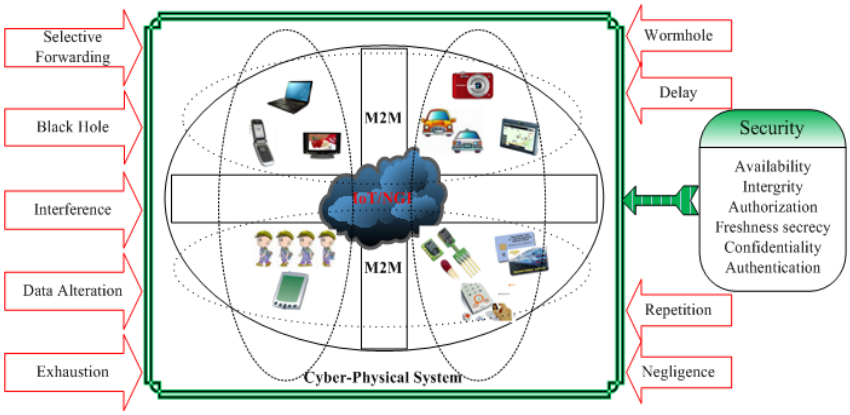

Fig. 1. Secure Issues in M2M communication in CPS

This paper focuses on several significant security issues with respect to availability, integrity, authorization, authentication and confidentiality. First, protect sensitive data and services from unauthorized internal and external access to CPS systems. Second, ensure some security principles for dynamic underlying infrastructures of CPS, such as confidentiality, integrity and authentication. Third, design novel individual authentication schemes with robust to the loss of packets during a transmission, short authentication latency and low computation. Last but not the least, protect privacy on the collected data from the physical world through scalar sensors, multimedia sensors, smart terminals, 3G phones, RFID readers and etc. Especially, privacy concerns arise beyond data content and may focus on context information in some M2M communications of CPS applications, such as the location of a sensor initiating data communication.

3. A Secure Architecture for CPS systems

With the development of WSNs, RFID and pervasive computing technology, CPS systems are becoming a reality. CPS applications have potential to benefit from massive wireless networks and smart devices. This allows CPS applications to provide intelligent services based on the knowledge from the surrounding physical world.

However, security and privacy issues must be addressed before CPS can be widely deployed in areas as diverse as military, financial, precision agriculture, assisted living, health

care and etc. To the best of our knowledge, the main reason why the security problem in CPS applications is so serious is that CPS systems usually involve interactions between the massive entities which may span heterogeneous wireless networks. Unlike other traditional network systems, CPS systems usually have no well-defined security perimeters. Furthermore, networks of CPS applications are usually wireless and dynamic in nature, including WSNs, Ad-Hoc network, Opportunistic Networks and etc.

In order to cope with the security issues discussed in Section 2, a secure architecture suitable for CPS applications is presented in this section, as shown in **Fig. 2**. The proposed secure architecture is also composed of four layers. In the perception layer, smart devices are connected into CPS systems to obtain sensitive data from their environment, including RFID Tags, 3G Phones, RFID sensors, sensors or sensor embedded devices and etc. We can employ lightweight key management schemes, secure routing protocols, intrusion detection systems and authentication schemes to cope with the security issues on availability, integrity and authentication. The network access layer can help heterogeneous networks to access Internet/NGI ubiquitously through a widely range wireless link, including Bluetooth, Wi-Fi, ZigBee, WiMAX, GSM, WCDMA, Satellite and etc. In this layer, mechanisms for data encryption, entities authentication and secure access can be used to protect privacy on the collected data from the physical world through scalar sensors, multimedia sensors, 3G phones, RFID reader and etc. The third layer is in charge of data management for CPS applications. In this layer, there are cloud computing centers, directory management severs, RESTful web servers and etc. And we can use SMC (Secure Multiparty Computation) based key distribution schemes to solve those security issues about confidentiality and freshness secrecy. The top layer provides various intelligent services to CPS users, such as precision agriculture, environment monitoring, intelligent transportation system and so on. Lightweight access control management mechanisms and privacy preserving technology can be used to cope with the problems concerning the authorization, confidentiality and freshness security of the transmitted data during the M2M communications in CPS. This secure architecture can detect: Black Hole, Selective Forwarding, Repetition, Delay, Data Alteration, Interference, Wormhole, Negligence, and Exhaustion.

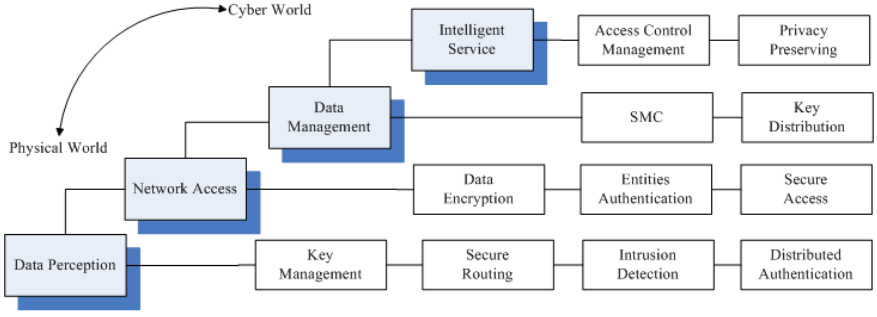

Fig. 2. The Secure Architecture of CPS

However, security policies and mechanisms developed for traditional applications are inadequate for CPS applications for several reasons. First, CPS applications are usually the integration of several heterogeneous wireless networks and do not have a well-defined security perimeter before deployed in physical world. In CPS systems, the entities which will be interacted with or the resources that will be accessed are not always known in advance. This makes almost all existing access control models unsuitable for CPS applications since they make access decisions based on the successful authentication of predefined users. Second, the

underlying networks of CPS are extremely dynamic in nature. The accessing entities may change, resources requiring protection may be created or modified and an entity's access to resources may change after deployed. Protecting resources during application execution remains challenging. Third, intelligent CPS applications are developed based on the knowledge of surrounding physical world. This requires security policies to use contextual information. Although, access to a resource may be contingent upon environmental contexts, such as the location and time which can be used to infer the activities of the user and even cause a privacy breach. Thus, the effects of physical security must also be considered when designing access control models in cyber world. Fourth, a CPS application may need to interact, cooperate and share resources with others to accomplish a given mission. Thus, secure interoperation in a dynamic network must be studied in-depth. Last, but not least, CPS often involves devices with various computation and communication capabilities, most of which are severely resource constrained. The resource constraints, such as limited battery lifetime, memory space and computing capability, make these nodes easy to attack and fairly hard to protect.

However, none of the existing work gives a set of corresponding countermeasures to cope with security issues involved in M2M communications of CPS clearly. This paper outlines the constrains and a set of challenges that need to be addressed for building secure CPS, and then proposes a more appropriate security architecture for CPS, eventually presents a survey of security and privacy preserving issues and the corresponding countermeasures in M2M communications. Security issues and countermeasures are classified into four categories: access control, intrusion detection, authentication and privacy preserving. Along the way we highlight the advantages and disadvantages of various security protocols and further compare and evaluate these protocols based on each of the four categories. We also point out the open research issues in each subarea and conclude with possible future research directions on security in CPS.

4. Security Issues and the Corresponding Countermeasures

4.1 Access Control

Access control is an essential security component to protect sensitive data and services from unauthorized internal and external access to CPS systems. However, existing access control policies and mechanisms are inadequate, and novel models and mechanisms are needed to protect such novel applications. CPS systems are different from conventional information processing systems in that they involve interactions between the cyber world and the physical world. Thus, securing such systems involve physical security, information systems security and, most importantly, interaction security between the physical world and the cyber world [14].

Different access control models have been proposed over the years. Among them, Role Based Access Control (RBAC) is gradually emerging as the standard for access control. Existing conventional access control models like RBAC are suitable for regulating access to resources by known users. S. Chakraborty etc. propose a trust based access control model called TrustBAC model [15]. It extends the conventional RBAC models with the notion of considering trust levels. As shown in **Fig. 3**, users are assigned to trust levels instead of roles based on several factors, like credentials, behavior, recommendation etc. However, these models have often been found to be inadequate for scalable and decentralized CPS systems where the user population is dynamic and the identities of all users are not known at all.

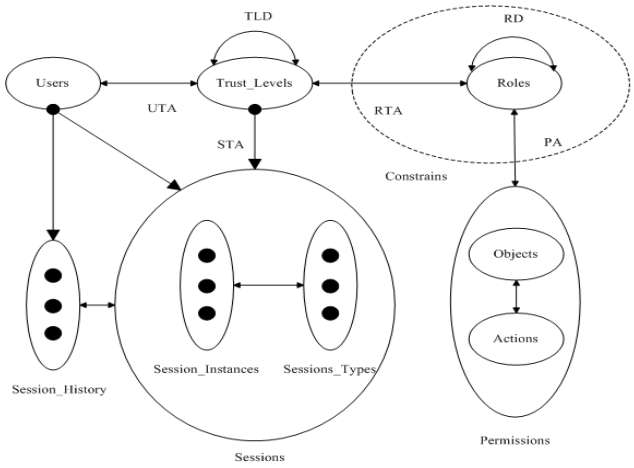

Fig. 3. The TrustBAC model

Spatial and temporal information for access can be employed to enhance the security for some mission-critical CPS applications. CPS computing applications are dynamic in nature and the set of users and resources are not known in advance. It is possible that a role for doing a specific task is temporarily unavailable and another role must be granted access during this time to complete it. I. Ray and M. Toahchoodee [16][17] propose a formal spatio-temporal model based on RBAC model that is suitable for commercial WSNs applications. They also show the association of each component of RBAC with spatio-temporal information and formalize the model by enumerating the constraints. This model can be used for those CPS applications where spatial and temporal information of a subject and an object must be taken into account before granting or denying access. However, the different features of a spatio-temporal access control model may interact in subtle ways resulting in conflicts. It is important to detect and resolve access control conflicts. M. Toahchoodee and I. Ray [18] illustrate how the access control model can be formally analyzed to detect the presence of conflicts and use a formal language Alloy based on first-order logic, for the purpose of convenient analysis. E. Helms [19] etc. propose an evaluating method to evaluate access control models of open source electronic health record systems for assisted living, and contribute the amalgamation of 25 criteria for the evaluation of access control implantation in the electronic health record system.

In order to accomplish the mission-critical application and fulfill its functionalities, a CPS system usually generates a large amount of data continuously over its lifetime. One of the biggest challenges in CPS systems is how to store and access these sensed data from the physical environment. Existing data storage and access strategies in CPS can be divided into two categories, namely, centralized and distributed approaches. Compared to the centralized case, distributed data storage and access consumes less bandwidth, since those sensed data is no longer forwarded to a centralized location out of the wireless network. Since a large amount of sensed data is distributedly stored and accessed in some individual sensor nodes, the corresponding data security issue becomes a serious concern in the wireless network of CPS. For those mission-critical applications, data sensed by the CPS network are closely related to security and privacy issues and accessed only by those authorized users. Especially, various types of data generated by different sensors may belong to different security levels, and should be accessed only by the selected types of users.

To address this challenge, S. C. Yu etc. [20] propose a Fine-grained Distributed data Access Control scheme, namely FDAC, specially tailored for the distributed wireless networks of CPS based on the continuous observation of the inherent nature of the sensor data. The proposed FDAC scheme is able to enforce fine-grained access control over sensor data and is resilient against strong attacks such as sensor compromise and user colluding. To our best knowledge, this paper is the first to realize distributed fine-grained data access control for CPS applications.

As discussed above, CPS can be affected by many security threats due to the open wireless communication channels. Therefore, it is necessary that only the authorized nodes can access the corresponding data. S. Misra and A. Vaish [21] propose a novel reputation-based role assignment for RBAC to evict highly non-cooperative and malicious nodes from wireless networks of CPS. A reputation management scheme is presented for multilevel hierarchical architecture in CPS based on the following three parameters: reputation, bootstrap time and energy.

The access control policies of these schemes are statically defined before the CPS application deployed, and cannot be adjusted according to the change of system environment dynamically. Especially in emergency situation, traditional access control schemes cannot provide proper privileges to execute the response actions to avoid the failure of the system. In CPS applications, physical environment is a key factor of the whole system when making the access control decisions, the environment context and the whole system context must be taken into account.

Emergency is defined as the effect of a series of events in physical world [22], which can cause the system to enter unstable states. G. W. Wu [23] etc. propose a new access control scheme called FEAC (Fault-tolerant Emergency-aware Access Control) which provides a proactive and adaptive access control policy specifically to address multiple emergency management problem and supposes a fault-tolerant scheme for CPS applications.

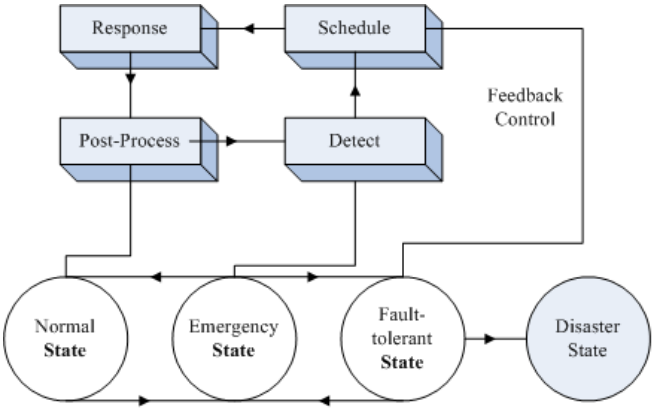

Fig. 4. The FEAC model

As shown in **Fig. 4,** in FEAC, the following five types of dependency relationships are considered, including entity dependency, time dependency, environment dependency, resource dependency and subject dependency. However, authorization and access control, which is often the first line of defense against security breaches, has not been addressed adequately in CPS.

Through the comparison of the current work (as shown in **Table 1**), we argue that access control for CPS systems mainly depends on the following factors: evaluation of the reputation

and trust of entities (such as trustworthiness), environmental context (such as location, time), and the specific context of the type of application. Note that, the most entities are held by smart devices themselves in CPS belong to the physical world and CPS networks always do not have well-defined security perimeters.

Table 1. A comparison of CPS access control models

Class	Basis	Scalable/decentralized
TrustBAC	Multi-Trust levels based RBAC	Weak
Spatio-temporal model based	Spatio-temporal model based RBAC	Weak
RRAS	Reputation-based RBAC	Normal
Detect/resolve control conflicts	Fault-tolerant Emergency-aware control policies	Normal
FDAC	Attribute-based encryption	Good
FEAC	Fault-tolerant theory based	Good

Therefore, we must integrate the effects of the above three factors into access control decisions in CPS applications. Trust is the connection between physical world and cyber world. The term ‘trust’ and ‘reputation’ have strongly linked meanings. Especially in WSNs of IoT/CPS, trust is often defined as an abstract of acquired attribute relative to some sensor nodes which is due to the amount of reputation held by such sensor nodes. By making full use of observing good long-term behavior, reputation ratings can be improved; therefore, trust relationships can be easily established. In real-life communities, trust is the consequence of the satisfaction of certain desired properties. The concept of reputation is closely linked to that of trust; however, there is a clear and significant difference. A node can trust in another node because of its good reputation. Likewise, a node can also trust in another node in spite of its bad reputation. Reputation is usually inspired by the past behaviors observed. Trust reflects the relying party’s subjective view of an entity’s trustworthiness, whereas reputation is a score which can be seen by the whole community. However, a lot of work remains to be done before such an access control model can be adapted for CPS applications.

4.1.1 Evaluation metrics of reputation and trust

Within the realm of IoT/CPS security, we interpret the concept of trust as a relation between entities (such as device, user, data, location and time) stored in sensor nodes that participate in various protocols. Trust relations are based on evidence or reputation created by the previous interactions of entities within a protocol. Each node employs a neighbor monitoring process in order to collect information about the packet forwarding behaviors of the neighbor nodes. Furthermore, each node is capable of overhearing the transmissions of its neighbors in the promiscuous mode. Each node independently overhears its neighboring nodes’ packet forwarding activities. This overhearing is related to the proportion of correctly forwarded packets with respect to the total number of packets to be forwarded during a fixed time window. Then, each node in the network maintains a data forwarding information table. The table includes only the data forwarding transaction information by overhearing its neighboring nodes. Eventually, we must propose a set of reasonable evaluation metrics of reputation and trust for CPS entities. Furthermore, based on these metrics, we can design a lightweight reputation and trust based access control model for CPS.

4.1.2 Group trust and secure execution

Trust research involves providing a formal basis that allows one to compare the different trust relationships that exist in CPS. Since multiple entities are involved in a CPS application, our research also needs to focus on how to compute group trust in a dynamic environment.

Although a lot of research focuses on security policies, not much of them can be directly applied to CPS applications. As mentioned above, traditional access control policies do not consider environmental contexts, such as location and time, when making access decisions. Traditional policies assume a very static configuration and the mechanisms enforcing these policies are relatively easy to implement. In CPS, the access control requirements change when the system context changes. Consequently, new notions of secure access control in the context of dynamic systems are needed. In short, the research task is to identify the types of policies needed in CPS and to propose a notion of secure execution for dynamic CPS applications.

4.1.3 Environmental contexts

Environmental contexts, such as location and time, play a crucial role in access decisions of CPS. Each application context generates a specific configuration of the system. We must firstly define what it means for access control protection in a given application context, and also ensure that security breaches do not occur while the application context is changed. For any given application context, the time and location of access together with the trustworthiness of the entities determine the access privileges of a user or a device. Note that, for a different application context, the privilege of this entity may change even if the other parameters (metrics of reputation and trust, location and time) remain the same. An access control model that captures all these requirements is needed for CPS.

4.1.4 Secure interoperation and policy conflict resolution

Under normal circumstances, these applications run independently. However, different CPS applications may need to interact and share resources to achieve a crucial universal mission. The issue involves how to formalize the notion of secure interoperation that takes into account such ad hoc interactions among individual applications. This will require identifying the threats that can occur because of the interactions and what types of policies are needed to protect against those types of breaches. In this situation, secure interoperation requires an application to operate under different sets of policies, including its own strategies and the universal strategies. Conflicts might occur because of the interaction of different policies. Further research is needed to identify how to detect and resolve these conflicts.

4.2 Intrusion Detection

Over the last few years, intrusion detection is regarded as a perfect weapon to cope with those challenges discussed above. The prevention mechanism is the first line of defense in a wireless network, ensuring some security principles, such as confidentiality, integrity and authentication for M2M communications of CPS. So far, there have been few works on the intrusion detection in CPS. However, there have been many useful results in the related fields, such as WSNs, Ad-hoc Network, and MANETs. Both of those networks do not have an underlying infrastructure and the topology is always changing over time, and the inherently vulnerable characteristics of wireless networks make them more susceptible to attacks from internal and external network. WSNs, Ad-hoc network, MANET and WSAN can be employed as underlying networks of CPS, since sensors, actuators, and RFID tags are the most effective tools for obtaining sensitive data from the physical world.

However, such networks employed by CPS present some new challenges when compared with traditional computer networks, namely in terms of smart node hardware constraints, very limited computing and energy resources. Unlike other networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, those functions are carried out by all available nodes. This significant difference is at the core of the

increased sensitivity to node misbehavior. The unreliability of wireless links between sensor/actuator nodes in the underlying networks of CPS applications, constantly leads to change topology due to the nodes movement in and out of the networks, resource constrains of underlying sensor/actuator networks employing ZigBee or 6LoWPAN communication protocols. Thus, it is particularly difficult to satisfy security requirements of CPS, notably because of the limited physical protection of each node, the sporadic nature of connectivity, and the absence of centralized certification authority. This fact is exacerbated by the nature of the deployed wireless networks. Often, nodes are deployed in a remote or hostile area, making them unprotected and susceptible to physical attacks [24].

Among the defense mechanisms, Intrusion Detection Systems (IDS) play important role in detecting attacks that can overcome the prevention techniques. Intrusion prevention is not guaranteed to work all the time and just works as a frontline security guarantee system which should detect an intrusion quickly enough. The solutions proposed in the literature generally fall into two main categories: prevention-based techniques and detection/retrieval techniques [25]. The standard procedure in an IDS is to compare the behavior of the current system with the normal behavior in the absence of any intrusions [26]. However, it is a hard task characterizing the normal behavior and normally it generates a great number of false positives. The second model, based on signatures, on the other hand, is based on known patterns of non-authorized behavior. The third approach, actually a combination of the previous ones, is called “specification based” [27]. As discussed in [28], the authors show why IDS solutions created for ad hoc wireless networks cannot be applied directly to sensor networks, and introduce the general guidelines for applying IDS architectures in static sensor networks (with no mobile nodes). In [29], the authors provide a solution to identify malicious nodes in WSNs through detection of malicious message transmissions in a network. The mechanism is proposed based on signal strength and geographical information for detecting malicious nodes staging HELLO flood and wormhole attacks. In [30], the authors propose a distributed IDS for WSNs based on groups. The wireless network is divided into several groups where each group is composed of sensor nodes which are close to each other and share the same capacity of sensing. And the IDS algorithm is executed in each divided group. In [31] the authors propose a decentralized IDS using the specification based approach, which can be adapted to a wide range of applications. The rules that can detect possible attacks related to the characteristics of WSNs nodes will be executed by the monitors spreading throughout the network in the packets sent by neighbor nodes. However, there are some problems in this work, such as not taking into account attacks to the monitors or the cooperation between the monitors. Through cooperation between the monitors, it is possible to obtain a correlation between the visions of each of the monitors, thus reducing the amount of false positives and negatives. In [32], the authors point out that the intrusion detection is usually defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. The design of intrusion detection modes considers two WSN models, including homogeneous and heterogeneous WSNs. The corresponding detection probability is derived by considering two sensing models, including single-sensing detection and multiple-sensing detection.

Traditional ways to secure a wireless networks are by using cryptographic techniques, safeguarding sensitive information from unauthorized access and implementing efficient intrusion detection mechanisms. [33] proposes a novel ant colony based intrusion detection mechanism which can keep track of the intruder trials. The proposed technique can also work in conjunction with the conventional machine learning based intrusion detection techniques to secure the WSNs. In [34], the research on intrusion detection focuses on an intruding packet in a communication network. Detection is accomplished by sampling a portion of the packets

transiting selected network links (or router interfaces). Since sampling entails incurring network costs for real-time packet sampling and packet examination hardware, it is advisable to develop a network packet sampling strategy to effectively detect network intrusions while not exceeding a given total sampling budget. A game theoretic framework is introduced to the proposed solution in **Fig. 5**, where the intruder picks paths (or the network ingress point if only shortest path routing is possible) to minimize the chances of detection and the network operator chooses a sampling strategy to maximize the chances of detection. The network intrusion game is played on the network between two players, including the service provider and the intruder.

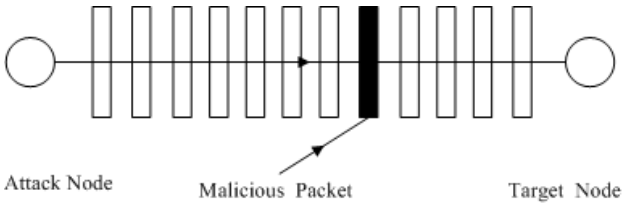

Fig. 5. The Intrusion Game Framework

The aim of an intruder is to inject a malicious packet form some attack node with the intention to attack a target node. If the malicious packet reaches the desired target node without detected by the proposed IDS, then an intrusion is successful. In order to detect and prevent the intrusion, the service provider is allowed to sample packets in the wireless network. If the service provider samples the malicious packet, then the intrusion is assumed to be detected and thwarted. The game theoretic problem is formulated and the corresponding sampling schemes are optimal in this game theoretic setting.

Table 2. A Comparsion of Existing IDSs

Class	Cooperation	Disadvantages
correlation-based	totally	all node involed, a learning phase
cluster-based	partially	reconstruction overhead, a learning phase
cooperative agent-based	totaly	all nodes involed, a learning phase
clustered agent-based	partially	reconstruction overhead

Obviously, some good ideas can be borrowed from these existing IDSs based on the comparison in **Table 2**. However, there are significant novel demands when these network infrastructures are introduced into the CPS applications. First, the nodes of CPS networks are not only sensors or sensor-embedded devices, but also actuators. The CPS applications usually need to give the feedback control to the target monitoring areas. This means that the data must be much more precise than that of WSNs, MANETs and so on. All these call for novel precise intrusion detection technology and intrusion detection models. Second, the wireless networks of CPS applications are usually heterogeneous. Traditional IDS and intrusion detection models are designed for homogenous networks. Since they lack this consideration when designing, the existing methods cannot be directly applied to ensure the security of CPS applications. Third, CPS applications are always mission-crucial. CPS applications are usually deployed in telemedicine/telehealth services, wearable e-health monitoring system and so on. These systems are so mission-crucial that cannot tolerate any security threats or malicious attacks. At the same time, the privacy of the data collected from individuals must also be preserved for the users. Consequently, we must investigate the security, privacy preserving

and reliability of CPS applications and propose some mission-oriented IDS for the wireless networks of CPS applications. Last but not the least, new challenges of security network access are introduced into wireless networks of CPS networks. Instead of ZigBee communication protocols, most of the wireless networks of CPS networks employ 6LoWPAN and Wi-Fi protocols in the underlying networks for data forwarding. Therefore, 3G, WiMAX, Satellite and GPRS etc. are used when accessing the IoT/NGI in order to exchange data between cyber world and physical world. When many access methods co-exist in a CPS network, how to ensure the access security of heterogeneous networks is an important issue. Since a large scale CPS application may span different heterogeneous wireless networks, during the design, the intrusion detection models should also consider the novel access security challenges which come with the emergence of CPS.

4.3 Authentication

Due to their unique nature, authentication in wireless networks in WSNs, MANETs and of CPS are challenging in the following ways: (1) The wireless nature of communication; (2) Resource (computing, storage, processing, protocol stack) limitation on sensor/actuator nodes; (3) Massive and dense sensors, sensor-embedded things, actuators, smart devices etc.; (4) Lack of fixed underlying infrastructure; (5) Dynamic topology, unknown network topology prior to deployment; (6) High risk of physical attacks on unattended sensors; (7) power consumption; and (8) Key management constraints.

In [35], the authors propose a novel light-weight authentication model based on the use of simple symmetric cryptographic primitives which overcomes the drawbacks presented above. By using a network-wide key for derivating pairwise keys in its initialization phase, the master key is no longer needed and it can be erased from the memory during the normal operation of the network. This approach may obtain the benefits of pairwise key schemes, i.e. node capture resilience, without the necessity of pre-distribution and storage of a large number of keys in each node. An authentication scheme for locating compromised or malicious sensor nodes in WSNs is proposes in [36]. The scheme is designed based on an intuitive observation for any well-behavior nodes in the wireless networks. And the set of outgoing messages should be equal to the set of incoming and locally generated messages. In this scheme, a provably secure incremental hash authentication scheme-AdHASH is employed to compare and locate malicious nodes.

As discussed in [37], a distributed WSN is usually a collection of low-end devices with wireless data exchange capabilities. It is a challenging problem to implement secure pairwise communications among any pair of sensors in WSNs. In particular, memory and energy consumption as well as resilience to sensor physical compromise are the most significant requirements. A pseudo-random key pre-deployment strategy ESP is also presented that supports an energy-efficient key discovery phase requiring no communications and provides node to node authentication.

In order to provide authentication, some utilize one way key chains and delayed disclosure of keys, others use one-time signature schemes. [38] proposes an efficient one-time signature-based broadcast authentication scheme to reduce storage usage and include a re-keying mechanism for WSNs. Though multi-level µTESLA schemes can scale up to large sensor networks (in terms of receivers), they either use substantial bandwidth and storage at sensor nodes, or require significant resources at the senders to deal with DOS attacks. In [39], the authors present efficient techniques to support a potentially large number of broadcast senders using µTESLA instances as building blocks. The proposed techniques are immune to the DOS attacks. This paper also provides two approaches, a revocation tree based scheme and

a proactive distribution based scheme, to revoke the broadcast authentication capability from compromised senders. Broadcast authentication is a critical security service in WSNs, as it allows the mobile users of WSNs to broadcast messages to multiple sensor nodes in a secure way. In [40], the authors argue that although symmetric-key based solutions such as μTESLA and multilevel μTESLA have been proposed, they all suffer from severe energy-depletion attacks resulting from the nature of delayed message authentication. The authors propose four different public key based approaches and provide in-depth analysis on their advantages and disadvantages. Several PKC-based schemes to address the proposed problem with minimized computational and communication costs are come up with. The goal is achieved by integrating several cryptographic building blocks, such as the Bloom filter, the partial message recovery signature scheme, and the Merkle hash tree, in an innovative manner.

In [41], the authors implement a user authentication protocol which is robust against node capture attacks. The protocol is based on elliptic curve cryptography and utilizes redundancy to withstand node capture. This protocol is the first step towards realizing authenticated querying in wireless networks of WSNs. This means that whenever the WSN processes a query, the sensor nodes should be able to verify that the query comes from a legitimate user. As there are potentially many users in the WSN, public key cryptography is used for user authentication, as it scales much better than symmetric cryptography approaches. The basic idea is to use sensors in the user's proximity as an interpreter between the "public key crypto world" of the user and the "symmetric crypto world" in WSNs.

In [42], User Authentication (UA) is considered for WSNs. Imagine that a wireless sensor network is deployed in an intelligent building, a hospital, or even a university campus, to allow legitimate users to send queries and retrieve the respective result at any of the sensor nodes. Importantly, the system needs to provide a means for user authentication to verify if the user is valid. The authors propose a dynamic strong-password based solution to this access control problem and adapt it into a wireless sensor network environment. The design of the proposed scheme making use of the security features on MAC sub layer (Medium Access Control) based on the IEEE 802.15.4 specification is presented. However, the scheme has three security weaknesses, as follows: (1) It cannot protect against the replay and forgery attacks; (2) Passwords could be revealed by any of the sensor nodes; (3) A user cannot change his/her password freely.

Therefore, in [43], the authors propose a lightweight dynamic user authentication scheme for WSNs. First, a user submits its user *uID* and the corresponding password in Hashed Form *H* (PW) to a *GW* (gateway) for registration. The *GW* stores the dataset (*uID, H (PW), TS*) in its database. Then *GW* replies to the user the successful registration. Eventually, the pair (*uID, TS*) is distributed to all the sensor nodes. Second, the user uses its password PW to compute a value *A=H (H (PW*) XOR t*), where t is the current time. Then, it submits the triple (*uID*, A, t*) to a login node. After receiving the login information, the login node first checks whether *uID** is in the list of datasets (*uID, TS*). If not, the login node sends a reject message to its user. Otherwise, it computes the value *C=H (A XOR T),* and sends *Msg(uID,C,T,t)* to the *GW* for authentication. Third, after receiving *Msg(uID,C,T,t)* from the login node, the GW first checks whether *(uID*, t)* is in its database. If *uID** is not in the database, the GW sends reject message to the login node. Otherwise, it computes *(H (H (PW) XOR t), H (H (H (PW) XOR t)) XOR T)* for verification. The *GW* verifies if *(C*=C)*. If so, the *GW* stores *t* in the database and sends an accept message to the login-node, and the user finally. Otherwise, the *GW* sends a reject message to the login-node. The proposed scheme is a modified scheme that not only retains all the advantages in the scheme presented in [42] but also enhances its security by withstanding the security weaknesses. However, an area of future research that should be considered is how

to achieve mutual authentication between the users and the sensor nodes. In addition, since there is a centralized *GW*-node in the proposed scheme, the performance in authentication might be improved by designing a decentralized *GW*-node.

In addition to the asymmetric models needed for broadcast authentication, the design of an efficient authentication scheme for M2M communications in CPS still faces many challenges.
(1) Robust to packet lost in wireless communication environment. Since the wireless networks of CPS applications are not reliable enough, the novel schemes of CPS must cope with the loss of packets during a transmission.
(2) Short authentication latency. Since most CPS applications are mission-crucial, real time response must be guaranteed, the maximum number of additional packets having to be received before a packet can be authenticated should be as small as possible.
(3) Individual authentication. The receiver should verify the received packets individually employing the authentication scheme without depending on other packets.
(4) Low computation, communication and storage overhead. Since the computation and storage overhead of a sensor node is so limited, some data (such as material and signatures) for authentication cannot be too large. Also, the number of bytes per packet used for authentication should be as small as possible.

4.4 Privacy Preserving

Much existing work on WSNs, MANETs and Ad-hoc networks is focused on addressing the power and computational resource constraints of sensors/actuators by the design of specific routing, MAC and cross-layer protocols. However, with the emergence of CPS and IoT, there have been recently heightened privacy concerns over the data collected by and transmitted through various wireless networks. Wireless transmission, the self-organizing nature, various heterogeneous nodes and feedback control makes privacy preserving in CPS an especially challenging problem.

In recent years, CPS has drawn considerable attention from the research community. What has received less attention, however, is the critical privacy protection on collected data from the physical world through sensors, smart devices, 3G phones, RFID reader and etc. As discussed in [44], privacy concerns arise beyond data content and may focus on context information, such as the location of a sensor initiating data communication. In some CPS applications, e.g. a remote e-health monitoring system, it is enough for an adversary to infer that the patient is suffering from a problem from the corresponding alert information and raw data which are collected from the patient's body and its physical environment.

Although there are many solutions proposed for wireless networks in WSNs, MANETs, ad-hoc networks, IoT and etc., and the underlying wireless networks of CPS have similar characteristics with these network infrastructures, the following inherent features of CPS introduce novel challenges to privacy preservation and prevent those existing techniques from being directly transplanted.
(1) Unpredictable environment. Sensors, sensor-embedded things, and actuators may have to be deployed in an environment unpredictable by the defender. The underlying things in CPS networks may vary from computation ability, storage ability and communication ability. Consequently, during the design period of a novel privacy preserving model, these issues must be fully considered.
(2) Heterogeneous networks. The wireless networks in CPS applications are always heterogeneous, even in one CPS application several wireless networks may be employed as the underlying network infrastructure.
(3) Node resource constraints. A battery-powered sensor, actuator or a sensor-embedded node

generally has severe constraints on its ability to store, process and transmit the sensed data. Therefore, the computational complexity and resource consumption of key management schemes are usually considered unsuitable for CPS applications.
(4) Topological constraints. The limited communication range of sensors or sensor-embedded things in a wireless network requires multiple hops to transmit data form the source. Especially, the deployment of actuators in a wireless network can be inferred to destroy the wireless network by the adversaries. Usually the feedback control process of a CPS application is affected by the data transmitted in the network. Tamper with raw data collected from the physical world or fusion data transmitted in the wireless traffic will cause catastrophic damage on the CPS application. Particularly, if an adversary holds the ability of global traffic analysis and observing the traffic of different sensor/actuator nodes over the whole network, it can easily compromise context privacy.

As discussed in [44], there are two main types of privacy concerns, data-oriented and context-oriented concerns. The former usually focus on the privacy data which are collected from a WSN or a query posted to a WSN (e.g. [45][46][47][48][49][50][51][52]). On the other hand, the latter concentrates on contextual information, such as the location and time in a WSN (e. g. [53][54][55][56]).

Data-oriented privacy protections focus on protecting the privacy of data content. There are two types of adversaries which may compromise data-oriented privacy. One is an external adversary which eavesdrops on the data communication between nodes in a wireless network. This type of adversary can be effectively relieved using cryptographic encryption and authentication. The other is an internal adversary which is a node captured and manipulated by malicious entities to compromise private information.

It is a challenging problem to provide efficient data aggregation while preserving data privacy in WSNs. In [45], two privacy-preserving data aggregation schemes are proposed for additive aggregation functions. The first scheme CPDA leverages clustering protocol and algebraic properties of polynomials. The second scheme SMART builds on slicing techniques and the associative property of addition. The goal is to bridge the gap between collaborative data collection by WSNs and data privacy. [46] proposes a set of generic, efficient and collusion-resilient privacy preserving data aggregation solutions. Based on the received histogram, the sink can then derive the approximate results of those particular queries such as MIN/MAX, Sum, Median, etc. Existing mechanisms for querying WSNs leak client interests to the servers performing the queries. The leaks are not only in terms of specific regions but also of client access patterns. In [47], the problem of preserving the privacy of clients querying a WSN owned by untrusted organizations is introduced. Then two architectures and the corresponding trust models are investigated. For the first model, consisting of multiple, mutually distrusting servers governing the network, an efficient protocol, SPYC, is designed to provide full query privacy. For the second model, where all queries are performed through a single server, two metrics for quantifying the privacy achieved by a client's query sequence are presented. [48] presents DP^2AC, a Distributed Privacy-Preserving Access Control scheme for WSNs, which is the first work of its kind. Users in DP^2AC purchase tokens from the network owner whereby to query data from sensor nodes which will reply only after validating the tokens. The use of blind signatures in token generation ensures that tokens are publicly verifiable yet unlinkable to user identities, so privacy-preserving access control is achieved.

To address source-location privacy for sensor networks, [49] provides a formal model for the source-location privacy problem and examines the privacy characteristics of different sensor routing protocols. Two metrics for quantifying source-location privacy in sensor networks are introduced. Then new techniques to enhance source-location privacy in routing

protocols are proposed. It is important that this privacy enhancement does not come at a cost of a significant increase in resource consumption. To preserve location privacy, [50] proposes to use source and sink-based random walk for packet delivery. The sink first sets up a path which serves as a receptor through random walk. Each packet from a source is then randomly forwarded until it reaches the receptor. At that point, the packet is forwarded to the sink through the pre-established path. A random walk greatly reduces the chance of packets being detected. Even if an eavesdropper happens to detect one packet, the next packet is unlikely to follow the same path, thus rendering the previous observation useless. [51] aims to provide source anonymity for sensor networks under a global observer who may monitor and analyze the traffic over the whole network. Every node in the network sends out dummy messages with intervals following a certain kind of distribution, e.g., constant or probabilistic. When a node detects a real event, it transmits the real event messages with intervals following the same distribution. As such, neither can an attacker discern the occurrence of a real event, nor can he find out the location of the real event source. Previous work has studied the source location privacy problem under a local adversary model. In [52], the authors solve the optimal proxy placement problem by using local search heuristics and propose a Proxy based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS), which are simple yet efficient event source unobservability preserving solutions for sensor networks. The two methods are designed to work together in order to maximally reduce the network traffic while increasing the delivery ratio without sacrificing privacy.

While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such information can be critical to the mission of sensor networks, such as the location of a target object in a monitoring application, and it is often important to protect this information as well as the message content. There are several recent studies on providing location privacy for sensor networks. However, these existing approaches assume a weak adversary model where the adversary sees only local network traffic.

As discussed in [53], a strong adversary model, the global eavesdropper, is often realistic in practice and can defeat existing techniques. Then the authors formalize the location privacy issues under this strong adversary model and show how much communication overhead is needed for achieving a given level of privacy. Two techniques that prevent the leakage of location information: periodic collection and source simulation are also proposed. Periodic collection provides a high level of location privacy, while source simulation provides trade-offs between privacy, communication cost, and latency. In [54][55], countermeasures are developed against traffic analysis attack which may seek to the base station or sink node, particularly the rate monitoring attack and time correlation attack. Four anti-traffic analysis techniques are presented to generate randomness.

Protecting the temporal privacy of a sensor network is a challenging issue, particularly as the concept of temporal privacy has not yet been formally defined. In [56], the authors address this need by providing a formal definition of temporal privacy that is built upon information theoretic concepts. In order to minimize the mutual information, a mechanism to buffer each packet at intermediate nodes along the routing path between a source sensor and the sink is also presented. The insights from the information-theoretic study further reveal that random delays that follow an exponential distribution will better protect temporal privacy than other distributions [57].

Although some techniques that can be introduced to CPS applications have been proposed in privacy protection in wireless networks of WSNs and Ad-hoc networks, there are still many open research issues in CPS. (1) The existing work only addresses systems with a single

mobile target. It is important to tackle the multiple mobile targets cases. Since most CPS applications employ multiple targets, some new privacy preserving models should be proposed. (2) CPS applications may employ the IoT/NGI as the backbone network, while WSNs, MANETs, etc. as the edge access networks. Obviously, the population of things connected to the IoT/NGI will be massive and grow rapidly because of the widespread application of 6LoWAN and IPV6 protocols. How to indentify the massive objects and protect the massive data privacy is still a challenging issue. (3) The privacy concerns of CPS applications are usually not only data-oriented but also context-oriented. Novel privacy preserving models should be proposed with in-depth consideration of the data privacy and contextual information privacy.

5. Future Research Directions

The previous section has identified the security issues in M2M communications of CPS systems. Although we have pointed out the open research issues in each subarea, we conclude with possible future research directions on security issues in CPS as follows: (1) A set of reasonable evaluation metrics of reputation and trust for CPS entities; (2) A lightweight reputation and trust based access control model for CPS; (3) New notions of secure access control in the context of dynamic systems; (4) Identifying the types of policies needed in CPS and proposing a notion of secure execution for dynamic CPS applications; (5) Environment context-aware access decision models; (6) Secure interoperation models of CPS systems; (7) A lightweight access control scheme to detect and resolve conflicts in security policies; (8) Secure precision feedback control intrusion detection models; (9) Novel intrusion detection systems for heterogeneous wireless networks in CPS; (10) Mission-oriented intrusion detection systems for CPS applications; (11) Packet loss tolerant authentication schemes for CPS; (12) SMC based lightweight authentication mechanisms; (13) SMC based privacy preserving techniques for CPS systems; (14) Data & context-oriented privacy preserving schemes; (15) Secure distributed massive data privacy protections; (16) Secure massive data storage and management mechanisms; (17) A secure heterogeneous wireless network fusion schemes; (18) Secure access network techniques for CPS; (19) Definition, evaluation and control of temporary privacy in CPS.

6. Conclusion

CPS aims at monitoring the behavior of physical processes, and actuating actions to change their behavior in order to make the physical environment work correctly. Nowadays, M2M has become an indispensable communication component and one of the frontiers for next generation networks, e.g. CPS, IoT. However, it is so difficult to enforce the M2M communication security of wireless networks, since massive smart terminals are expected to be deployed in highly heterogeneous distributed CPS networks. In this paper, a survey of security and privacy preserving issues of M2M communications in CPS is given. First the constrains, attack issues, and a set of challenges that need to be addressed for building secure CPS systems are presented, and a universal security architecture for M2M communication in CPS systems is proposed. Then, security issues and the corresponding countermeasures are further discussed. Security issues and countermeasures are classified into four categories: access control, intrusion detection, authentication and privacy preserving. In this paper, we give a detailed analysis and summary of the related works systematically and deeply, and then point out the research thinking and methods based on the novel characteristics of CPS systems

from the four aspects. Eventually, we summarize possible future research directions on security in CPS.

However, there are still other good countermeasures to cope with these security and privacy issues, such as key management, secure routing, data encryption, SMC based key distribution schemes or mechanisms. We will continue to investigate these countermeasures in the future. And this paper gives the survey of security issues in M2M communications in CPS systems based on insufficient actual CPS applications. We will also investigate more typical CPS applications and improve the research on security in M2M communications of CPS further.

References

[1] W. Wolf, "Cyber-physical system," *Computer*, vol. 42, no. 43, pp. 88-89, 2009. Article (CrossRef Link)

[2] R. Poovendran., "Cyber-physical systems close encounters between two parallel worlds," *Procedding of the IEEE*, vol. 98, no. 8, pp. 1363-1366, 2010. Article (CrossRef Link)

[3] W. Yong, G. Atteburyn and B. Ramamurthy, "A survey of security issues in wireless sensor networks", *Communications Surveys & Tutorials*, IEEE, vol. 8, no. 2, pp. 2-23, 2006.Article (CrossRef Link)

[4] D. Djenouri, L. Khelladi and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *Communications Surveys & Tutorials*, IEEE, vol. 7, no. 4, pp. 2-28, 2005.Article (CrossRef Link)

[5] E. K. Wang, Y. M. Ye, X. F. Xu, et al., "Security issues and challenges for cyber physical system," in *Proc. of 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber-Physical and Social Computing (CPSCom)*, pp. 733-738, Dec. 2010. Article (CrossRef Link)

[6] M. Anand, E. Cronin, M. Sherr, et al., "Security challenges in next generation cyber physical systems," in *Proc. of Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and*, Nov. 2006. Article (CrossRef Link)

[7] E. A. Lee, "Cyber physical systems: design challenges," in *Proc. IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, 2008. Article (CrossRef Link)

[8] C. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *Proc. of 20th Tyrrhenian International Work-shop on Digital Communications*, pp. 389-395, Sep.2009. Article (CrossRef Link)

[9] R. Weber, "Internet of things-new security and privacy challenges," *Computer Law & Security Review*, vol. 26, pp. 23-30, 2010. Article (CrossRef Link)

[10] C. Inhyok, Y. Shah, A. U. Schmidt, et al., "Security and trust for M2M Communications," *Vehicular Technology Magazine, IEEE*, vol. 4, no. 3, pp. 69-75, Sep. 2009. Article (CrossRef Link)

[11] A. A. Cardenas, S. Amin and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS2008)*, pp. 495-500, Jun. 2008. Article (CrossRef Link)

[12] M. Saedy and V. Mojtahed, "Ad Hoc M2M Communications and security based on 4G cellular system," *Wireless Telecommunications Symposium (WTS)*, pp. 1-5, Apr.2011. Article (CrossRef Link)

[13] C. Inhyok, Y. Shah, A. U. Schmidt, et al., "Trust in M2M communication," *Vehicular Technology Magazine, IEEE*, vol. 4, no. 3, pp. 69-75, Sep. 2009. Article (CrossRef Link)

[14] R. Indrakshi and R. Indrajit, "Access Control Challenges for Cyber-Physical Systems". Article (CrossRef Link)

[15] S. Chakraborty and I. Ray, "Trust BAC-integrating trust relationships into the RBAC model for access control in open systems," in *Proc. of the 11th ACM Symp. on Access Control Models And Technologies*, New York: ACM Press, pp. 49-58, 2006. Article (CrossRef Link)

[16] I. Ray and M. Toahchoodee, "A spatio-yemporal access control model supporting delegation for pervasive computing applications," in *Proc. of the 5th International Conference on Trust, Privacy and Security in Digital Business*, pp. 48-58, Sep. 2008. Article (CrossRef Link)
[17] I. Ray and M. Toahchoodee. "A spatio-temporal role-based access control model," in *Proc. of the 21stAnnual IFIP TC-11 WG 11.3 Working Conference on Data and Applications Security*, pp. 211-226, Jul. 2007. Article (CrossRef Link)
[18] C. M. Jonker and J. Treur, "Formal analysis of models for the dynamics of trust based on experience," in *Proc. of the 9th European Workshop on Modeling Autonomous Agents in a Multi-Agent System Engineering*, pp. 221-232, Jul. 1999. Article (CrossRef Link)
[19] E. Helms and L. Williams, "Evaluating access control of open source electronic health record systems," in *Proc. of the 3rd workshop on Software engineering in health care*, pp. 63-70, 2011. Article (CrossRef Link)
[20] S. Yu, K. Ren and W. Lou, "FDAC: Toward Fine-grained Distributed Data Access Control in wireless sensor networks," in *Proc. of IEEE INFOCOM 2009*, pp. 963-971, 2009. Article (CrossRef Link)
[21] S. Misra and A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks," *Journal of Computer Communications of Elsevier*, vol. 34, no. 3, pp. 281-294, 2010. Article (CrossRef Link)
[22] S. K. S. Gupta, T. Mukherjee and K. Venkatasubramanian, "Criticality aware access control Model for pervasive applications," in *Proc. of the 4th IEEE Conference on Pervasive Computing and Communications*, pp. 251-257, 2006. Article (CrossRef Link)
[23] G. W. Wu, D. Z. Lu, F. Xia, et al., "A fault-tolerant emergency-aware access controls scheme for cyber-physical systems", in *Proc. of Information Technology and*, vol. 40, no. 1, pp. 29-39, 2011. Article (CrossRef Link)
[24] H. Alzaid, E. Foo and J. G. Nieto, "Secure data aggregation in wireless sensor network: a survey," in *Proc. of the 6th Australasian Information Security Conference*, ACSC2008, pp. 93-105, Jan. 2008. Article (CrossRef Link)
[25] B. Parno, E. Gaustad, M. Luk, et al., "Secure sensor network routing: a clean-slate approach", in *Proc. of CoNEXT 2006*, pp. 1-13, 2006. Article (CrossRef Link)
[26] R. Shorey, A. Ananda, M. C. Chan, et al., "Mobile, wireless, and sensor networks: technology, applications, and future directions", *John Wiley & Sons. Hoboken*, 2006. Article (CrossRef Link)
[27] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using specification-based intrusion detection for automated response," in *Proc. of 6th International Symposium Recent Advances in Intrusion Detection*, pp. 136-154, 2003. Article (CrossRef Link)
[28] R. Roman, J. Zhou and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proc. of the 3rd IEEE Consumer Communications and Networking Conference*, pp. 640-644, 2006. Article (CrossRef Link)
[29] W. R. Pires Jr., T. H. P. Figueiredo, H. C. Wong, et al., "Malicious node detection in wireless sensor networks," in *Proc. of the 8th International Parallel & Distributed Processing Symposium (IPDP'04)*, pp. 24-27, 2004. Article (CrossRef Link)
[30] G. R. Li, J. S. He and Y. F. Fu, "A distributed intrusion detection scheme for wireless sensor networks," in *Proc. of the 28th International Conference on Distributed Computing Systems Workshops*, vol. 0, no. 0, pp. 309-314, 2008. Article (CrossRef Link)
[31] A. P. R. Silva, M. H. T. Martins, B. P. S. Rocha, et al., "Decentralized intrusion detection in wireless sensor networks," in *Proc. of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pp. 16-23, 2005. Article (CrossRef Link)
[32] Y. Wang, X. Wang, B. Xie, et al, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698-711, Jun. 2008. Article (CrossRef Link)
[33] S. Banerjee, C. Grosan, A. Abraham, et al., "Intrusion detection on sensor networks using emotional ants," *International Journal of Applied Science and Computations*, vol. 12, no. 3, pp. 152-173, 2005. Article (CrossRef Link)

[34] M. Kodialam and T. V. Lakshman, "Detecting network intrusion via sampling: a game theoretic approach," in *Proc. of IEEE INFOCOM 2003*, vol. 3, pp. 1880-1889, 2003. Article (CrossRef Link)
[35] O. D. Mohatar, A. F. Sabater and J. M. Sierra, "A lightweight authentication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 727-735, 2010. Article (CrossRef Link)
[36] Y. T. Zhang, J. Yang, W. J. Li, et al., "An authentication scheme for locating compromised sensor nodes in WSNs", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp.50-62, Jan. 2010. Article (CrossRef Link)
[37] R. D. Pietro, L. V. Mancini, A. Mei, et al., "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", *ACM/Kluwer Wireless Networks*, vol. 12, no. 6, pp. 709-721, 2005. Article (CrossRef Link)
[38] S. Chang, S. Shieh, W. W. Lin, et al., "An efficient broadcast authentication scheme in wireless sensor networks", in *Proc. of ACM Symposium on Information, Computer and Communications Security*, pp. 311-320, 2006. Article (CrossRef Link)
[39] D. Liu et al., "Practical broadcast authentication sensor networks," in *Proc. of 2nd Annual Int'l. Conf. Mobile and Ubiquitous Systems: Networking and Services*, pp. 118-29, Jul. 2005. Article (CrossRef Link)
[40] K. Ren, W. Lou and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in *Proc. of 4th Annual IEEE Communications Society Conference on Sensor, Meshand Ad Hoc Communications and Networks*, pp. 223-232, 2007. Article (CrossRef Link)
[41] Z. Benenson, N. Gedicke and O. Raivio, "Realizing robust user authentication in sensor networks," in *Proc. of Workshop on Real-World Wireless Sensor Networks*, 2005. Article (CrossRef Link)
[42] K. Wong et al., "A dynamic user authentication scheme for wireless sensor networks," in *Proc. of IEEE Int. Conf. Sensor Network, Ubiquitous*, Trustworthy Computing, pp. 244-251, 2006. Article (CrossRef Link)
[43] H. R. Tseng, R. H. Jan and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. of IEEE Global Telecommun. Conf.*, pp. 986-990, 2007. Article (CrossRef Link)
[44] N. Li, N. Zhang, S. Das, et al., "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Journal of Ad Hoc Networks*, vol. 7, no. 8, pp. 1501-1514, Nov. 2009. Article (CrossRef Link)
[45] W. B. He, X. Liu, H. Nguyen, et al., "PDA: Privacy-preserving Data Aggregation in wireless sensor networks," in *Proc. of INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, pp. 2045-2053, 2007. Article (CrossRef Link)
[46] W. Zhang, C. Wang and T. Feng, "GP2S: generic privacy-preservation solutions for approximate aggregation of sensor data," in *Proc. of 6th IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 179-184, 2008. Article (CrossRef Link)
[47] B. Carbunar, Y. Yu, W. Shi, et al., "Query privacy in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 2, pp. 1-34, 2010. Article (CrossRef Link)
[48] R. Zhang, Y. Zhang and K. Ren, "DP2AC: Distributed privacy-preserving access control in sensor networks," in *Proc. of INFOCOM 2009*, pp. 1251-1259, 2009. Article (CrossRef Link)
[49] P. Kamat et al., "Enhancing source location privacy in sensor network routing," in *Proc. Int'l Conf. Distributed Computing Systems*, pp. 559-608, 2005. Article (CrossRef Link)
[50] Y. Xi, L. Schwiebert and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proc. of the 20th International Parallel and Distributed Processing Symposium*, pp. 8-18, 2006. Article (CrossRef Link)
[51] M. Shao, Y. Yang, S. Zhu, et al., "Towards statistically strong source anonymity for sensor networks," in *Proc. of the 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, pp. 51-55, 2008. Article (CrossRef Link)
[52] Y. Yang, M. Shao, S. Zhu, et al., "Towards event source unobservability with minimum network traffic in sensor networks," in *Proc. of the first ACM conference on Wireless network security*, pp. 77-88, 2008. Article (CrossRef Link)

[53] K. Mehta, D. Liu and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. of IEEE International Conference on Network Protocols*, pp. 1536-1233, 2007. Article (CrossRef Link)
[54] S. Mishra J. Deng and R. Han, "Countermeasures against traffic analysis attacks in wireless sensor networks," *Technical Report CU-CS-987-04*, Dec. 2004. Article (CrossRef Link)
[55] J. Deng, R. Han and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Journal of Pervasive and Mobile Computing on Security in Wireless Mobile Computing Systems*, vol. 2, no. 2, pp. 159-186, 2006. Article (CrossRef Link)
[56] P. Kamat, W. Xu, W. Trappe, et al., "Temporal privacy in wireless sensor networks". *ICDCS '07:* in *Proc. of the 27th International Conference on Distributed Computing Systems*, pp. 23-24, 2007. Article (CrossRef Link)
[57] J. F. Wan, H. H. Yan, H. Suo, et al., "Advances in Cyber-Physical Systems Research," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 11, pp. 1891-1908, Nov.2011. Article (CrossRef Link)

Dong Chen received his master degree in Computer Science in July 2010 at Northeastern Univ., China. Now, he is a Ph.D. candidate in Computer Science at Northeastern Univ. His main research interests are Cyber-Physical Systems and Internet of Things.

Guiran Chang is a Professor at Northeastern Univ., China. He received his bachelor degree in 1970 from Tsinghua Univ. and his Ph.D. degree in 1991 from the Univ. of Tennessee. His research interests include: Wireless Sensor Network, Cyber-Physical Systems, and Cloud Computing.