Journal of Theoretical and Applied Information Technology
20th January 2015. Vol.71 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBER SECURITY FOR CYBER PHYSCIAL SYSTEMS: A TRUST-BASED APPROACH

[1]SAQIB ALI, [2] RAJA WASEEM ANWAR and [3]OMAR KHADEER HUSSAIN

[1] Department of Information Systems, Sultan Qaboos University, Sultanate of Oman

[2] Faculty of Computer Studies, Arab Open University, Muscat, Sultanate of Oman

[3] School of Business, The University of New South Wales, Canberra, Australia

E-mail: [1]saqib.ali@ieee.org , [2]waseem@aou.edu.om, [3]O.Hussain@adfa.edu.au

ABSTRACT

Cyber- Physical Systems (CPS) consist of a combination of different embedded subsystems, which work independently of each other and also interact with the external environment. Such embedded systems operate in the presence of inherent uncertainty, context dependencies and adversarial certainty arising from both the cyber and physical worlds. Security is one of the key concepts to shield the CPS environment and different embedding devices in order to have a reliable and secure communication platform. There are many security approaches and methods proposed and implemented globally in order to secure CPS, along with areas such as social engineering, security standards, vendor control, as well as access control implementation, etc. However, in addition to these areas, another important concept, namely trust, is significant in ensuring secure and reliable communications in CPS. In the current state-of-the-art, none of the existing approaches discusses the issue of a secure, trust-based CPS. Thus, to address this shortcoming, in this paper, a two-tier blanket approach is proposed consisting of internal and external layers of trust among different entities to create reliable and secure CPS. This trust-based framework improves the confidence of secure entities joining the CPS system and also builds relationships among entities, thereby increasing the security protecting the formed CPS from outside threats and attacks.

Keywords: *Cyber-Physical Systems, Trust, Security, SCADA, Embedded Systems*

1. INTRODUCTION

Over the last few years, there has been a tremendous increase in the number and variety of computers for everyday use. Modern computers are becoming smaller and smaller, but capable of much higher performance in terms of computational speed and memory size, as predicted by Moore's law. As a consequence, computers are being transformed into smaller items such as mobile phones, smart sensors and similar physical objects. In other words, many physical things now possess different levels of computing and communication capabilities, which are provided by miniature and invisible computers embedded therein. This integration of networked computing and physical dynamics has led to the development of Cyber-Physical Systems (CPS), which have become very popular in recent years [18].

CPS are closely integrated and developed using computational, networking, and physical objects. In CPS, embedded devices are used in the network to sense, monitor, control and observe the physical world. A CPS creates a connection between the cyber and physical world. It offers two kinds of services; physical services offered by the physical units and cyber services accessible by software systems in the CPS [1]. A classic CPS model mainly includes physical units or objects, sensors, communication networks, actuators and computing devices which are distributed and directly knitted with physical entities communicating with each other through the CPS network. The communication network can either be a small area-specific network or a mixture of multiple wired or wireless networks. These networks are responsible for transmitting sensor-collected information reliably in real-time and send back to the controller. All computing devices operate through complex decision-making algorithms that help in generating

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

control commands for different objects or devices, based on the information collected by sensors [2]. CPS have enormous applications in a wide variety of systems, including medical systems, industrial monitoring, agriculture and avionics [3]. With the broad expansion of WSN devices and due to the massive growth in pervasive computing, the growth and adoption of CPS is expected to rise in the future [13]. A conceptual map developed by the Berkeley Cyber-Physical Systems Group [25] clearly identifies the key components of a CPS.

The development of CPS provides advanced and flexible communication options, making CPS vulnerable to security attacks in both local and external domains. External threats include eavesdropping on the communication channel, channel modification and jamming, etc. [1]. Local threats are threats from inside users, such as disrupting the functionalities of the network. Local threats in which malicious devices join the network to disrupt the communication operations of the CPS are difficult to detect using conventional security functions due to limitations of power and memory [2]. A common secure communication platform in CPS is vital to combat these threats.

One way to address local threats in CPS is to have an authentication process to prevent such malicious nodes from joining the network. A variety of techniques to establish authentication in CPS have been developed to ensure that a new user joining the group will not cause any security issues. Trust in this context ensures that the security and reliability of the network will not be compromised after a particular user is permitted to join the network. Such a trust-based authentication mechanism will allow only non-malicious nodes to access the CPS network resources thus safeguarding the whole CPS against outside threats. Even though the literature survey highlights the importance of trust during the process of authentication, a suitable framework in which users are authenticated prior to joining the network, has not yet been proposed. Thus, this paper aims to fill this gap in CPS security and proposes such a framework based on trust. A trust relationship between different nodes of the CPS creates a platform to address difficult security issues and provide secure communication between different nodes. Nevertheless, malicious nodes may attack the key nodes of the CPS (sensors or actuators), forcing the degradation of the network's performance or even taking it offline. Hence, it is important to find a way to wed trust and security for a stronger CPS. To prevent such occurrences, this research proposes a framework to automatically reconfigure the CPS in the event of such an attack.

A CPS is classified into two main domains: a cyber-infrastructure consisting of virtual or cyber objects and a physical infrastructure consisting of physical objects. These systems are designed and developed to support efficient resource utilization, control, performance and fault tolerance. The main feature of the embedded system in the CPS is to control both the physical appearance and cyber computations. CPS security is dealt with independently to the cyber and physical world. Access control and information flow-based methods are the two main approaches to system security policies and mechanisms [19].

2. BACKGROUND AND LITERATURE REVIEW

Cyber-Physical Systems have been developed and expanded over the last couple of years due to the advances in embedded wireless technology and pervasive computing.

In [6], the authors introduce secure cyber-physical wireless sensor networks (WSNs) integrating cloud computing for u-life care architecture called (CPeSC3). CPeSC3 architecture consists of a communication core, a computation core, resource scheduling and a management core. The security core consists of a source sensor node with a random number encrypted to provide protection against attacks. The research focuses on how to enhance secure wireless sensor networks, and integrate them in cloud computing.

In [7], the authors propose a lightweight, hardware-based security technique for CPS. They consider the use of Physically Unclonable Functions (PUFs) to bind an access request to specific hardware with device-specific keys. These PUFs use SRAM in the implementation of hardware to identify the devices. Location-based access control and encryption can be achieved by using this technology as one of the desirable objectives of CPS. This work considers hardware-based techniques to enhance CPS device-based performance, which is one of the major areas in CPS, but again there is no discussion or inclusion of a trust component in CPS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In [8], the authors propose an access control scheme called fault-tolerant emergency-aware access control (FEAC). The FEAC control scheme provides adaptive and proactive access control policies. These policies are designed to address the problems of managing multiple emergencies and providing support to fault-tolerant schemes for CPS applications. In [8], the authors also introduced the Priority and Dependency-Action Generation Model (PD-AGM). This model selects the optimal response action path, eliminating all the active emergencies within the system. The priority and dependency relationships of emergencies are addressed for the combination state explosion problem. This research discusses the issues related to proactive and adaptive access control policies based on the integration of software and hardware-based systems. However there is a lack of attention to major security issues related to trust-based CPS.

In [9], the authors develop three novel software methodologies to provide improved security in embedded real-time systems. The three software methodologies are T-Rex, T-Prot and T-Axt which detect more intrusions that harm security in CPS. This work concentrates more on software-based techniques to enhance security in real-time embedded systems.

In [10], the authors propose a six-layer security architecture for CPS. This architecture is derived from the OSI and PRM models. A holistic approach towards security solutions in CPS is adopted, discussing the presence of security issues at each layer of the six-layer security architecture. The authors also propose a game-theoretical model developed from the physical layer and stressed that a saddle-point solution to the dynamic game gives rise to a cross-layer security policy. Although a layer-based security approach is adopted which ensures security at each layer within the system, nothing is suggested or discussed in relation to trust.

In [11], the authors propose a method for security risk assessment called Bayesian Attack Graphs (BAGs) which integrates the usual cause-consequence relationships between diverse network states considering the likelihood of the exploitation of such relationships. The Common Vulnerability Scoring System (CVSS) is the metrics employed to estimate an organization's security risk from different vulnerability exploitations. This research concentrates on vulnerabilities and the likelihood of the exploitation of these vulnerabilities using a Bayesian attack graph.

In [12], the authors describe a framework for information systems assessment while considering uncertainty. The authors adopt different architectural scenarios to analyze cyber security through a model-based assessment framework. Bayesian statistics-based Extended Influence Diagrams are used in the framework to express attack graphs and related countermeasures. The model, merged with Meta models using a concept called Abstract models, is beneficial for analyzing different architectural scenarios.

Based on the literature review and analysis, it is evident from the initial findings that most of the studies target a specific area of security, but do not consider issues associated with trust, which is vital both for the present and in the future. In CPS, security should be included as an integral part of the CPS architecture and application development rather than simply applying security solutions [4]. Security issues within CPS applications must be addressed due to the nature of and interaction with the physical environment [8]. The following sub-section discusses a few of the common attacks in CPS:

2.1 Different types of attacks in CPS:

Designing, implementing and maintaining CPS is difficult because of the number of possible cyber-security attacks. Some of the common attacks in CPS are discussed as follows [5]:

Eavesdropping

In this type of attack, the opponent can intercept the data or any information communicated by the system. In CPS sensor networks transferring monitoring data to the CPS, applications can become vulnerable to eavesdropping. Eavesdropping also violates the user's privacy in the case of being monitored using such systems.

Compromised-Key Attack

In this type of attack, an attacker can hold a compromised key to gain access over the secured communication without the awareness of either sender or receiver. The attacker can perform modifications on the captured data using the compromised key, and perform additional

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

computational steps to gain access to other secure keys based on the compromised key.

Man-in-the-Middle Attack
This type of attack involves a third person sending fabricated messages to the recipient, and can take the form of false negative or false positive messages. Upon receiving such messages, the recipient takes certain actions, such as controlling the basic functions of the cyber physical systems.

Denial-of-Service Attack
This type of attack prevents the system from responding to legitimate requests from the network resources and performing normal processes. Attackers can use such an attack to gain access over the system to flood a controller to force it to shutdown, change the behavior characteristics of the system and/or block traffic to make the network unavailable.

Resonance attack
In this attack, sensors or controllers are compromised and forced to operate at a different resonant frequency [12].

Communication Jamming attack
In a communication jamming attack [26], a sensor node communicates with a remote station through a wireless channel which might be jammed by an external attacker and results in early depletion of sensor nodes due to energy constraints.

Integrity attack
In this type of attack in CPS, an attacker wishes to disrupt the system by injecting external control inputs and fake sensor measurements [27].

2.2 Threats/uncertainties and protection of assets in Cyber-Physical Systems:

Like any other system, security is a key challenge for the deployment of CPS. CPS need protection from threats that, in turn, exploit any vulnerability and cause damage to the CPS.

Information systems consist of software, hardware, services, people, data, etc. and are referred to as assets. Information systems are always susceptible to a number of threats. Threats can be classified as hardware and software, physical, operational, service related, management related, applications, modifications, falsifications and repudiation, etc. [20].

In [20], the researchers focus on the three main challenges of securing CPS: understanding the threats and possible setbacks of attacks; identifying the exclusive properties of CPS in relation to other IT security issues; and discussing the security mechanisms applicable to CPS. Proofread

In order to understand the threats related to the smart grid and SCADA (Supervisory Control and Data Acquisition Systems) within CPS, it is useful to classify the interactions based on the domain, the origin of the threat, and its impact [21].

One major characteristic of cyber threats is that they are scalable, automated, replicated and propagated freely across untrusted domains. Cyber threats include disrupting the integrity and confidentiality of data, including connecting to a device on a network and retrieving usage data or modifying information etc. Cyber-physical threats have an impact on the physical characteristics of a system.

Today's CPS need strong information and communication abilities. Due to the vulnerability of pervasive communications, new approaches and technologies will be required to enhance the protection of power system command, control and communication [22].

3. NEED FOR TRUST-BASED SECURE CYBER-PHYSICAL SYSTEMS

Currently, CPS are an emerging and growing category of systems that combine physical systems with computational logics/techniques in a holistic way [23]. The main characteristics include functionality and relevant system properties which appear from the rigorous interaction of computational and physical components. Computational components within CPS are intrinsically distributed, (time)-synchronizing and designed to cope with the uncertainty of sensor input and real-time interactions.

CPS are normally designed as networks of interacting elements, some examples being medical monitoring systems, process control systems such as Smart Grid, SCADA systems, automotive systems and distributed robotics.

Journal of Theoretical and Applied Information Technology
20th January 2015. Vol.71 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Due to this integration of CPS and embedded systems, challenges arise between the two (cyber and physical) domains in establishing trust and security.

Currently, there are no defined procedures for the evolving trust-based security threats and asset identification of CPS.

Due to the growing complexity of components and the use of progressive technologies for sensors and actuators, wireless communication poses the foremost challenge in CPS. There is a lack of security awareness among employees. Hence, organizations need to adopt greater security-consciousness and awareness by educating and training employees in corporate security policies.

3.1 Significance

Within the growth of pervasive computing, CPS gain importance as they can largely be applied to different domains within the cyber-physical world. The potential applications of CPS include factory automation, home automation, traffic control systems, integrated medical services, automotive systems, critical infrastructure control, research and rescue systems, environmental controls, distributed autonomous robotics, and so on. These services and applications can vastly improve quality of life [2].

3.2 Trust and Security in CPS

Trust is a complex concept and is defined in many different ways [16]. In [20] , trust is defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". Many people relate trust with security although security, on its own, does not require the presence of trust. There are many different ways by which online trust can be established [21, 22, 23, 24]. According to [22], the level of security does not affect trust, as security is not a component of trust. Under the umbrella of e-commerce, security is co-related with trust due to the concept that more online security measures will increase the level of trust of those who are willing to engage in e-commerce as the user's data i.e. personal details including credit card numbers are being protected [23, 24].

In today's world, trust is introduced to address certain problems. Commonly, trust is understood as a trusted opinion, reputation and/or probability. In this case, trust is considered as the probability that a CPS object will perform the required actions.

In classic security models, a security perimeter is defined to create a trust boundary. Trust and security are two closely related, dependent concepts used when establishing a secure system [17, 34]. But establishing trust is complex and incurs high overheads.

Many researchers have focused on trust for many years in diverse domains, from the social sciences to economic transactions [35 – 38]. It is very important to understand the concept of trust to model it properly in CPS security.

CPS are also being employed in estimation and control algorithms to satisfy certain operational goals such as safety, optimizing the performance function, and closed-loop stability. Security is needed to safeguard infrastructure from cyber-attacks [14] and non-operational objectives collected by the sensor network containing private information. It is very important to meet confidentiality, integrity and availability requirements.

4. TRUST-BASED SECURE CPS APPROACH

A trust-based two-tier secure cyber-physical-oriented system approach is proposed as follows:

Internal Trust for different internal trusted entities such as sensors, actuators and communication networks.
External Trust for the physical environment or the architecture of CPS.

Achieving trust in CPS is very tiresome and challenging; in this proposed approach, the boundary of trust is created internally and externally around CPS, as depicted in Figure 2.

The integration of these two levels of trust will be achieved by implementing a two-tier blanket approach, where the blanket covers the whole CPS and hides it from the outside world. The proposed approach's integration and coordination issues are clearly defined, achieved and analyzed.

Journal of Theoretical and Applied Information Technology
20th January 2015. Vol.71 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

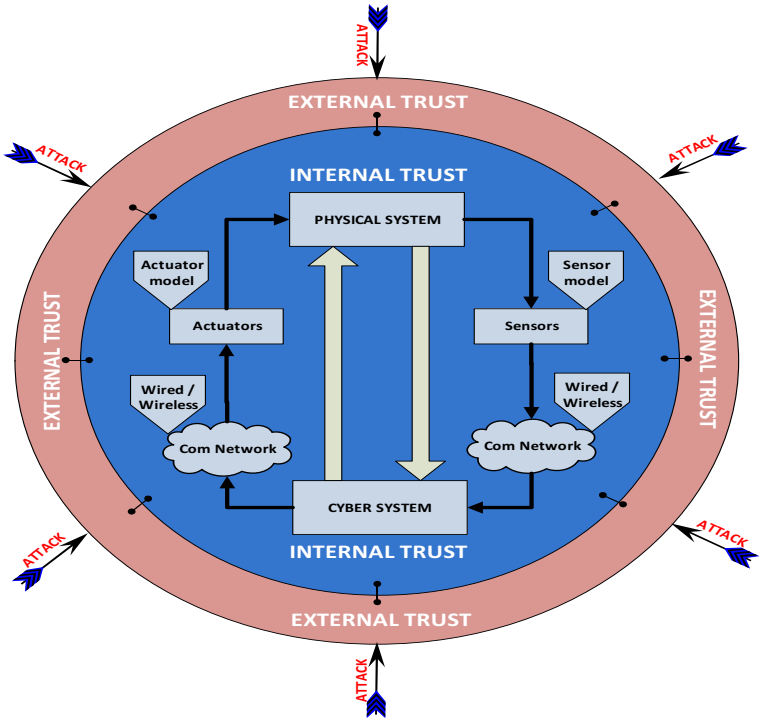

Fig. 2 Trust-Based Secure CPS Approach

CPS differ from user-based computing to wireless sensor-based networks due to their defining characteristics.

The CPS components interconnected on a large-scale perform autonomous task execution to link cyber systems with physical systems [28].

The following are the main components of the proposed trust-based CPS approach and an explanation of their roles:

- Physical System: A collection of actuator units.
- Sensors and actuators: To monitor and measure various physical processes. They create the interface between both physical and cyber domains. Sensors normally measure physical characteristics e.g. oil well temperatures and converts this into relevant information [29].
- Communication Network (wired / wireless): To provide a connection between cyber and physical systems.
- Cyber System: To control logic, sensor units and critical infrastructures.
- Internal Trust: To trust physical systems, sensors and actuators and internal communication networks.
- External Trust: To state internal trust and external entities.
- Boundary: The parameterized boundary where trust is established.
- Attacks: All kinds of external attacks on CPS.

Trust is an important concept with respect to security. Trust refers to the behavior and a belief that a specific entity will produce a specific or desired result and will work in a predictable manner under specified circumstances.

Establishing trust between internal and external components in any CPS is challenging due to the growing concern over cyber-attacks targeting these infrastructures. One major limitation of today's CPS is the lack of an established threat model to characterize the security needs and the level of acceptable risk.

Trust Management and Attribution [29]: The cyber infrastructure in the power system domain can be viewed as interconnected "islands of automation' which raise inherent trust concerns. In addition, if an organization has a system affected by a security event, then this information might not be communicated to all concerned domains. Therefore,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

decreased trust is not appropriately communicated to all other systems.

- Trust Management Lifecycle: The dynamic environment of the smart grid requires a trust model which allows continual re-evaluation. As the smart grid exhibits emergent behaviors, trust management must remain flexible to address continual modifications in usage and misuse patterns.

- Insider Threat Management: To prevent nefarious actions by the employees which can result in disastrous results.

- Attribution: The ability to attribute actions back to a system or user is imperative in order to identify malicious actors. By developing strong attribution mechanisms, the individuals responsible for a cyber-attack can be identified and penalized, deterring future malicious activities.

In addition to the above, this study has identified several issues which could strongly influence the establishment of trust among CPS components, which include but are not limited to the following:

- Technical implications
- Practical implications
- Management implications
- Access control to vendors
- Standardization: (up to what extent)
- Vender influence
- Weakest link (people working for a particular organization)

Nowadays, CPS is critical for Information and Communication Technology (ICT) services as it facilitates the automated and efficient management of vital services. It is mandatory to ensure these systems are secure in relation to all kinds of attacks.

According to [5], a highly confident CPS should satisfy the following objectives, in addition to trust, which this research considers as another important objective.

Confidentiality:
Preventing unauthorized access to or disclosure of an individual's information is very important in CPS to preserve a user's privacy and confidentiality. Confidentiality in CPS must be ensured to prohibit an attacker from eavesdropping on a communication channel between the controller, sensor and actuator.

Integrity:
Integrity refers to the assurance that data or resources cannot be modified by unauthorized users and it is therefore trustworthy. The primary goal of CPS is to prevent and detect attacks on the information communicated between sensors, actuators and controllers.

Availability:
Ensuring the continuous availability of CPS services without any disruption is one of the primary objectives of information security. In order to achieve this, it is necessary to prevent communication failures, hardware failures, power outages and DoS attacks.

Authenticity:
During communication between autonomous networks in CPS, it is necessary to authenticate the data, transactions and communications.

Trust Oriented:
According to [15], trust is context-dependent (trust relationships are only meaningful in specific contexts), dynamic, non-monotonic and a function of uncertainty.

Types of Trust:
- Interpersonal (agent & context-specific)
- Structural (system within which trust exists)
- Dispositional (independent of agent & context)

Trust is important when building a relationship between entities. Different domains use different modeling and calculation techniques to examine trust. Statistics and probability are common techniques used in dynamic networks where the topology is changing rapidly to examine the modeling and calculation of trust.

CPS consist of integrated and embedded components (sensors, actuators, communication network). Trust-based CPS should have common communication with each other to understand security attacks and countermeasures in a trusted way. In this research, a two-tier blanket approach is adopted that provides a common platform for both humans and software agents to share and understand information about information security.

5. CONCLUSION

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In order to achieve secure CPS, the trust factor needs to be taken into account and incorporated at the very start of the process of designing such systems. CPS are creating new avenues for research and development in many disciplines. This research highlights a key area: the lack of trust in securing CPS. The incorporation of trust in CPS to achieve security is still an unresolved and challenging issue. This research presented a two-tier, trust-based blanket approach to achieve security in CPS.

This research will be further extended to implement a trust-based approach to determine the extent to which this research has succeeded in securing CPS. This research will also analyze the existing security mechanisms in CPS in comparison with trust-based CPS.

ACKNOWLEDGMENTS

The research leading to these results has received research project grant funding from the Research Council of the Sultanate of Oman Research Grant Agreement No [ORG SQU ICT 13 011].

REFERENCES:

[1] W. Kaiyu and V. Alagar, "Dependable Context-sensitive Services in Cyber-Physical Systems", *International Joint Conference of IEEE TrustCom-11*, Nov 16-18 , 2011,pp. 687 - 694.

[2] F. Xia, A. Vinel, R. Gao,L. Wang and T. Qiu, "Evaluating IEEE 802.15.4 for Cyber-Physical Systems", *EURASIP Journal on Wireless Communications and Networking*, 24 Dec 2013.

[3] John A. Chandy, "Managing Information and Storage in Networked Cyber-Physical Systems", *National Science Foundation Workshop on Cyber-Physical Systems*, September 8, 2006.

[4] K. K. Fletcher and X. Liu, "Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber- Physical Systems", *Fifth IEEE International Conference on Secure Software Integration and Reliability Improvement – Companion*, 27-29 June 2011 ,pp. 106 – 113.

[5] E. K. Wang, Y. Ye, X. Xu, S.M.Yiu, L.C.K.Hui and K.P.Chow, "Security Issues and Challenges for Cyber-Physical System", *IEEE/ACM International Conference on Green Computing and Communications & IEEE/ACM International Conference on Cyber, Physical and Social Computing*, 18-20 Dec. 2010, 733 - 738.

[6] J. Wang, H. Abid, S. Lee, L. Shu and F. Xia, "A Secured Health Care Application Architecture for Cyber-Physical Systems", *Control Engineering and Applied Informatics*(13/.3), 31 Dec 2011, pp. 101-108.

[7] M. Kirkpatrick, E. Bertino and F. T. Sheldon, "Restricted Authentication and Encryption for Cyber-physical Systems", *DHS CPS Workshop Restricted Authentication and Encryption for Cyber-physical Systems*, 2009.

[8] G. Wu, D. Lu, F. Xia and L. Yao, "A Fault-Tolerant Emergency-Aware Access Control Scheme for Cyber-Physical Systems", *Information Technology and Control* (40/ 1), 31 Dec 2011 ,pp. 29-44.

[9] C. Zimmer, B. Bhat, F. Mueller and S. Mohan, "Time-Based Intrusion Detection in Cyber-Physical Systems", *Proceedings of the first ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS '10)*, April-13 2010, pp.109-118.

[10]Q. Zhu, C. Rieger and T. Basar, "A Hierarchical Security Architecture for Cyber-Physical Systems", *IEEE 4th International Symposium on Resilient Control Systems (ISRCS)*, 9-11 Aug. 2011,pp. 15 - 20.

[11]N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", *IEEE Transactions on Dependable and Secure Computing(9/1)*, Jan.-Feb. 2012 ,pp. 61 - 74.

[12]T. Sommestad, M. Ekstedt and P. Johnson, "Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models", *Proceedings of the 42nd Hawaii International Conference on System Sciences, (HICSS)*, 2009.

[13]NSF Workshop on Cyber-Physical Systems, http://varma.ece.cmu.edu/cps/, Oct. 2006

[14]Alvaro A. Cardenas, S. A. "Secure Control: Towards Survivable Cyber-Physical Systems." *The 28th International IEEE Conference on Distributed Computing Systems Workshops* , 17-20 June 2008 ,pp. 495 - 500.

[15]M. Blaze., J. Feigenbaum and J. Lacy, "Decentralized Trust Management". *Proceedings of IEEE Symposium on Security and Privacy*, 6 May 1996, pp. 164-173.

[16]"A survey of Trust Management Systems", Dalal Al-Arayed , Supervised by: Joao Pedro Sousa, PhD Asisstant Professor, CS, GMU

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[17]S. Pearson, A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", *In Proceedings of 2nd IEEE International Conference on Cloud Computing Techology and Science*, Nov. 30 2010-Dec. 3 2010 , pp. 693-702,.

[17]M. Momani, S. Challa, "Survey of Trust Models in Different Network Domains", 1 Oct 2010.

[18]T. T. Gamage, B. M. McMillin, T. P. Roth. "Enforcing Information Flow Security Properties in Cyber-Physical Systems: A Generalized Framework Based on Comoensation", *34th Annual IEEE Computer Software and Applications Conference Workshops* , 19-23 July 2010 ,pp. 158 - 163.

[19] Z. Xinlan, H. Zhifang, W. Guangfu and Z. Xin. ."Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarachy Process", *Second IEEE WRI World Congress on Software Engineering(2),* 19-20 Dec. 2010 , pp. 157 - 160.

[20]C. Neuman, K. Tan. "Mediating Cyber and Physical Threat Propagation in Secure Smart Grid Architectures", *IEEE International Conference on Smart Grid Communications* , 17-20 Oct. 2011, pp. 238 - 243

[21]S. M. Amin, D.Sc, "Toward Smarter and More Secure Power and Energy Infrastructures", *Canada – U.S Workshop on Smart Grid Technologies*, March-25-2010.

[22]H. Giese, B. Rumpe, B. Schatz and J. Sztipanovits , "Science and Engineering of Cyber-Physical Systems", *Dagsthul Reports* (1/ 11), pp 1-22.

[23]Gilbert, Nigel and Terna, "How to build and Use Agent-Based Models in Social Science". *Mind and Society*, (1/1), pp.57 – 72, 2000.

[24]"Cyber-Physical Systems, website", [online], Available: http://cyberphysicalsystems.org/index.html

[25]Guirguis, Emad, "On The Effect Of Jamming Attacks On Cyber-Physical Systems With The Focus On Target Tracking Applications" (2012). https://digital.library.txstate.edu/handle/10877/2458

[26] Yuzhi Li, Ling Shi, Peng Cheng, Jiming Cheng and Daniel E. Quevedo , "Jamming attacks on Cyber-Physical Systems: A Game-theoretic approach", *Proceeding of the 2013 IEEE International Conference on Cyber Technology in Automation*, Control and Intelligent Systems May 26 – 29, 2013, Nanjing, China http://dl.acm.org/citation.cfm?id=2185514

[27] Y. Tan, M. C. Vuran and S. Goddard "Spatio-Temporal Event Model for Cyber-Physical Systems", *CSE conference and workshop papers*, 22-26 June 2009,pp. 44 – 50.

[28]Cyber-Physical Systems Security for Smart Grid (Future Grid Initiative White Paper), PSERC Publication February-2012.

[29]F.Xia and J. Ma (Natural Science Foundation of China Grant Number: 60903153, the fundamental Research Funds for Central Universities (DUT10ZD110), and the SRF for ROCS, SEM), Building Smart Communities with Cyber-Physical Systems.