IoT Security Framework for Smart Cyber Infrastructures

Jesus Pacheco, Salim Hariri
Electrical and Computer Engineering Department
The University of Arizona
Tucson, Arizona, USA
{jpacheco, hariri}@email.arizona.edu

Abstract— **The Internet of Things (IoT) will connect not only computers and mobile devices, but it will also interconnect smart buildings, homes, and cities, as well as electrical grids, gas, and water networks, automobiles, airplanes, etc. IoT will lead to the development of a wide range of advanced information services that need to be processed in real-time and require data centers with large storage and computing power. The integration of IoT with Cloud and Fog Computing can bring not only the required computational power and storage capacity, but they enable IoT services to be pervasive, cost-effective, and can be accessed from anywhere using any device (mobile or stationary). However, IoT infrastructures and services will introduce grand security challenges due to the significant increase in the attack surface, complexity, heterogeneity and number of resources. In this paper, we present an IoT security framework for smart infrastructures such as Smart Homes (SH) and smart buildings (SB). We also present a general threat model that can be used to develop a security protection methodology for IoT services against cyber-attacks (known or unknown). Additionally, we show that Anomaly Behavior Analysis (ABA) Intrusion Detection System (ABA-IDS) can detect and classify a wide range of attacks against IoT sensors.**

Keywords—internet of things; threat model; attack vector; cyber security; smart infrastructures; fog computing.

I. Introduction

Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services will lead to the development of the next generation of Internet services (Internet of Things (IoT)) that are pervasive, ubiquitous, and touch all aspects of our life. It is expected that the number of IoT devices will reach more than 50 billion devices by 2020 [1]. The IoT services will be a key enabling technology to the development of smart cities that will revolutionize the way we do business, maintain our health, manage critical infrastructure, conduct education, and how we secure, protect, and entertain ourselves [2]. The integration of physical and cyber systems as well as the human behaviors and interactions (e.g., producers, consumers, and attackers) will dramatically increase the vulnerability and the attack surface of interdependent infrastructure ecosystems. The most common architecture to monitor and control smart infrastructures such as Smart Homes (SH) and Smart Buildings (SB) are Building Automation Systems (BAS) and Supervisory Control and Data Acquisition (SCADA) systems. As BAS and SCADA systems become interconnected with Internet resources and services, they become easy targets to cyber adversaries, especially since they were never designed to handle cyber threats; they were designed to operate in a completely isolated environment from corporate networks and the Internet. This makes control system data vulnerable to falsification attacks that lead to incorrect information delivery to users, causing them to take wrong and dangerous actions or to be unaware of an attack underway, as was the case with Stuxnet attack [3]. It also allows adversaries to potentially execute malicious commands on control systems and remote devices, causing harmful actions. Therefore, it is critically important to secure and protect the IoT operations of such systems against cyber-attacks.

In this paper, we first introduce our IoT security framework for Smart Homes that consists of four layers: devices (end nodes), network, services, and application. Then the attack vector that can be launched against each layer is analyzed. We present a methodology to develop a general threat model in order to better recognize the vulnerabilities in each layer and the possible countermeasures that can be deployed to mitigate their exploitation. We develop an ABA-IDS to detect anomalies that could be triggered by attacks against the sensors of the first layer. We have evaluated our approach by launching several cyberattacks (e.g. Sensor Impersonation, Replay, and Flooding attacks) against our Smart Home testbed developed at the University of Arizona Center for Cloud and Autonomic Computing. The results show that our IoT security framework can be used to develop security mechanisms to protect the normal operations of each layer. Moreover, our approach can detect known and unknown attacks for IoT end nodes, with high detection rate and low false alarms.

The rest of the paper is organized as follows. In section II we provide background information about the concepts of smart infrastructures and SH, IoT cyber security, Abnormal Behavior Analysis IDS, and the use of a threat model. In Section III, we explain our IoT security framework for SH. In section IV, we present our experimental environment and discuss our evaluation results. In section V, we conclude the paper and discuss future research direction.

II. Background

A. Smart Infrastructures, Cloud and Fog Computing

Smart Infrastructures (SI) integrate autonomy and adaptive control and can be considered as the next generation of smart and automated infrastructures. SI links industrial controllers, automation, information technology, sustainable development, security, and communications (among other systems) to

978-1-5090-3651-6/16 $31.00 © 2016 IEEE
DOI 10.1109/FAS-W.2016.58

achieve advanced information services that reduce operational cost, improve human comfort and reduce energy consumption [4][5]. Because of the wide range of users, interconnected systems and environmental factors, the computational power needed to operate SIs is similar to that needed in large scale data centers. Cloud and Fog Computing can provide a cost-effective, scalable, and ubiquitous alternative solution to traditional data centers. Cloud Computing provides computing, storage, and applications as services that are offered on demand in a cost-effective and a scalable way. Resources can be shared among a large number of users, who can access applications and data from anywhere at any time [6]. On the other hand, Fog Computing aims at providing computational power, storage, and network services to end devices. Since Fog computing host services at the network edge, its advantages include low service latency, high quality services, support for mobility, location awareness, and easier implementation of security mechanisms. It has been shown that Fog computing can be effective in supporting IoT applications that demand predictable latency [7].

B. *IoT Cyber Security*

IoT can be viewed as a ubiquitous network that enables monitoring and controlling a large number of heterogeneous devices that are geographically dispersed by collecting, and processing and acting on the data generated by smart objects [8]. It represents intelligent end-to-end systems that enable smart solutions and covers a diverse range of technologies including sensing, communications, networking, etc. [8]. This diverse and dynamic use of resources have made security a major challenge. Traditional IT security solutions are not directly applicable to IoT due to the following issues: [8]: 1) The IoT extends the "internet" through the traditional internet, mobile network, non IP networks, sensor network, cloud computing, and fog computing; 2) Computing platforms, constrained in memory and processing capability and consequently may not support complex security algorithms; 3) All "things" will communicate with each other. This leads to multiple access points that can be used to exploit existing vulnerabilities; and 4) Some IoT devices and services may be shared and could have different ownership, policy, and connectivity domains.

These challenges need to be addressed in order to build a secure and resilient IoT infrastructure, where Confidentiality, Integrity, and Availability (CIA) must be assured. Consequently, there is a strong research interest in securing and protecting SI and their services using resilient techniques [9].

C. *Abnormal Behavior Analysis*

Current cyber-security solutions are far from being satisfactory to stop the exponential growth in number and complexity of cyber-attacks [10]. In addition, the effort and knowledge required to launch sophisticated attacks is decreasing while their propagation has been reduced from days in the early 80s to a fraction of seconds in 2000s. There are two basic intrusion detection techniques to detect cyberattacks: signature based and anomaly based Intrusion Detection Systems (IDS) [11]. Signature based IDS builds a database of known attack signatures. However, these systems cannot detect new types of attacks. The main feature of the anomaly detection approaches is their capability in detecting novel and new attacks. The Anomaly Based IDS defines a baseline model for normal behavior of the system through off-line training, and consider any activity which lies outside of this normal model as anomaly [12]. Any attack, misconfiguration or misuse will lead to deviation from the normal behavior; we name it as Abnormal Behavior. The main limitation of this approach is the large number of false alarms that can be produced. Our approach overcomes this limitation by performing fine grain anomaly behavior analysis as will be discussed in further detailed when we introduce our ABA-IDS approach.

D. *Threat model*

Improving security and reducing risks in information systems depend heavily on analyzing threats, risks and vulnerabilities in order to develop the appropriate countermeasures to mitigate their exploitations [13]. In order to better understand the IoT security landscape, a general IoT threat model needs to be developed [14][15]. A threat model defines threat scenarios with associated risk distributions. It helps in analyzing a security problem, design mitigation strategies, and evaluate mitigation solutions. When created in the design phase, a threat model helps to identify changes that need to be made to the design to mitigate potential threats. When a threat model is created for a deployed system, it can be used to prioritize the mitigation actions [13][16]. In general the steps to create a general threat model are: 1) Identify attackers, assets, threats and other components, 2) Rank the threats, 3) Choose mitigation strategies, and 4) Build mitigation solutions based on the strategies.

III. IoT Security Framework for Smart Infrastructures

There are several IoT frameworks that can be used to create a threat model and apply mitigation strategies [7][17][18][19][20]. Figure 1 shows an architecture that can be used to guide the security development of IoT smart infrastructures. The frameowrk consists of four layers: IoT end Nodes (end devices), Network, Services and Applications.

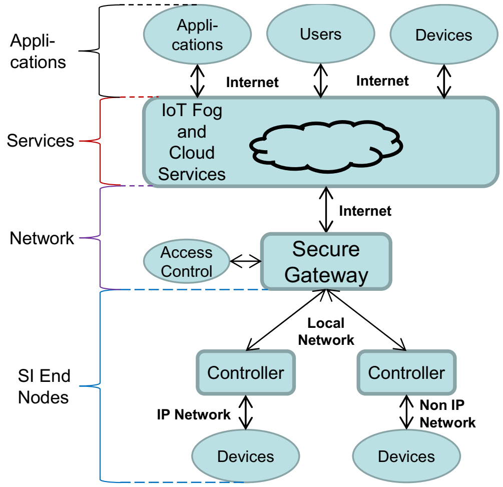

Fig. 1. IoT security framework for Smart Infrastructures

Cyberattacks can be launched against the functions and services provided by each layer shown in Figure 1. For each layer in our framework we can define the threats in terms of target, impact, and mitigation methods.

In the first layer (end nodes) the information passes through physical devices to identify the physical world. This information includes object properties, environmental conditions, data, etc. The key components in this layer are the sensors for capturing and representing the physical world in the digital world, and the actuators to modify the environment to a desired state. Target at this level are local controllers, sensors, actuators, and information. The impact can be energy waste, money, human safety, provider's reputation, and waste of time. Mitigation mechanisms include lightweight encryption, sensor authentication, IDS, anti-jamming, and behavior analysis.

Network layer is responsible for the reliable transmission of information from/to end nodes [20]. The technologies used in this include the Internet, mobile communication networks, wireless sensor networks, network infrastructures, and communication protocols. Network security and management play an important role to defend against cyber-attacks targeting firewalls, routers, protocols, and personal information. The impacts might be in money, reputation, safety, energy, control, and time. Network mitigation mechanisms include authentication, anti DoS, encryption, packet filtering, congestion control, anti-jamming, intrusion detection, and behavior analysis.

The services layer acts as an interface between the application layer in the top level and the network layer in the lower level [19]. At this layer, all the required computational power is mostly provided as a cloud service. In this layer, cyberattacks target personal and confidential information, IoT end devices, monitor and control functions. The impact includes people safety, money losses, and important information leakage. Protection mechanisms include encryption, authentication, session identifiers, intrusion detection, selective disclosure, data distortion, and behavior analysis.

The application layer provides the personalized services according to the needs of the user [20]. The access to the IoT services is through this layer and it can be via mobile technology such as cellphone, mobile applications, or a smart appliance or device. In this layer, data sharing is an important characteristic and consequently application security must address data privacy, access control and information leaks. The impacts are stolen intellectual properties, disclosure of critical business plans, money loss, and damaging business reputation. Some mitigation mechanisms include encryption, authentication, and anomaly behavior analysis of applications and their services.

Attackers may use any existing vulnerability to gain access to the system and launch an attack. Our framework can be used to identify the potential vulnerabilities and the appropriate mitigation mechanism. For instance, an IP temperature sensor located in a remote place can be easily replaced by a computer to obtain illegal information and to launch an attack (e.g. replay attack). Since sensors usually have low (or no) computational power, it is unrealistic to apply encryption techniques, a more suitable approach is to authenticate each sensor and its data.

A. *Attack Surface*

Attacks on a system take place either by launching an attack within the system's operating environment (insider attack) or by launching it from an external source (outsider attack) [21]. In both cases, an attacker will use the system's resources (methods, channels, and data) to launch attacks. We consider two sides of the IoT network, one for local network (insiders) and one for public networks (outsiders) [22]. Local networks include end devices, IP and non-IP networks, controllers, and gateways. Public networks include IoT services, and applications. The IoT security architecture shown in Figure 1 can be used to derive the attack surface shown in Table 1.

TABLE I. ATTACK SURFACE FOR SI IN IOT

Location	**Attack surface**
Inside (local network)	Device to Device Door ⇔ Alarm
	Device to Controller Controller ⇔ Lights
	Controller to Gateway Command ⇔ Service
	User to Gateway Authentication ⇔ Access
Outside (public network)	User to IoT services User ⇔ Stored data
	Service to service Health care ⇔ Payment
	Application to service Smart Home ⇔ Electricity
	IoT device to service Smart phone ⇔ Fog data

B. *Smart Home Testbed (SHT)*

The SH testbed has all the characteristics and functionalities of the actual smart homes such as sensors, actuators, automation systems, and communication channels. In our testbed, the user can monitor Smart Building (SB) variables and control elements using a variety of protocols (e.g. ZigBee, Wi-Fi, and BACnet). Variables include temperature, distance, motion, current, humidity, and illumination. The elements to control are lights, ventilators, door, and electric sockets. The monitor and control tasks can be performed locally by accessing our secure gateway, and remotely by using fog or cloud services. The SHT will enable us to experiment with and evaluate different security mechanisms, and resilient algorithms and study their impacts on normal SH services.

IV. ABNORMAL BEHAVIOR ANALYSIS METHODOLOGY

We have developed strategies to protect the operations of end nodes against any type of threat by using continuous monitoring and performing anomaly behavior analysis of the end nodes operations. The main modules to implement our approach are shown in Figure 2: 1) Continuous Monitoring, 2) Data structure, 3) Anomaly Behavior Analysis, 4) Sensor Classification, and 5) Recovery Actions.

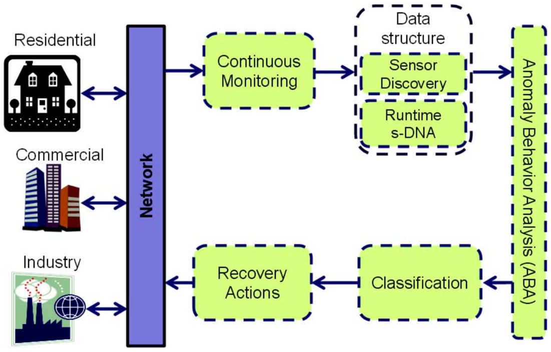

Fig. 2. Methodology for ABA for sensors

A. Continuous monitoring

We have used software tools to capture the behavior of SHT components that are important to characterize their normal operations. For example, we use Wireshark monitoring tool to capture the required sensor operational data [24]. The information obtained from Wireshark includes source IP, destination IP, and content of packets. The sensor's data is extracted from the payload and sent to the Data Structure module, where the sensor is automatically identified and its runtime profile. We refer to the sensor profile as the Sensor-DNA data structure (s-DNA) that is built by using Discrete Wavelet Transform (DWT) method.

B. Data Structure

This module performs two tasks: 1) Compute the DWT coefficients form the signal, and 2) Identify sensor type based on received data to create the runtime profile that will be compared with the reference s-DNA in the ABA module.

1) DWT coefficients

The data obtained from the sensor is decomposed using DWT method as shown in Equations (1) and (2). In each level of the decomposition, the extracted coefficients are used to build the s-DNA data structure which is used by the ABA module.

$$y_{high}[k] = \sum_{n} x[n] * g[2k - n] \tag{1}$$

$$y_{low}[k] = \sum_{n} x[n] * h[2k - n] \tag{2}$$

The original signal *x[n]* is decomposed into an approximation coefficient $y_{high}[k]$, and a detail coefficient $y_{low}[k]$ by applying a high pass *g[n]* and a low pass *h[n]* filters respectively. The number of samples in the signal follow $n=2^i$ form. The DWT can be computed efficiently in a linear time, which is important when dealing with large datasets. We use Haar wavelet as the function to extract the coefficients because any continuous function can be approximated with this function [23]. Once the signal is decomposed, the coefficients of each level are aggregated in a single vector that is used to build the s-DNA data structure.

2) Sensor classification

The next step is to identify the sensor type based on the received data. For this task, the Euclidean distance D_j in Equation (3) is computed between the runtime coefficient vector $\boldsymbol{v}$ and a matrix $\boldsymbol{M}$ of coefficients obtained during the offline training phase.

$$D_j = \sqrt{\sum_{i=1}^{n} \left(M_{i,j} - v_i \right)^2} \tag{3}$$

The smallest distance obtained is used to classify the sensor type. Once the sensor type has been identified, the rest of the data is compared with the coefficients in the same column (*j*) of the matrix to obtain the Euclidean distance.

C. Abnormal Behavior Analysis

The Euclidean distance is compared with the reference model in the ABA. The reference model is built during the offline training by using normal measurement attributes (normal Euclidean distance). Five vectors are used to find the control limits for normal operation [24]. Each vector is compared with the rest. Once all the distances are computed, the mean value (CL) is calculated from the samples. The Upper Control Limit (UCL) and the Lower Control Limit (LCL) for the normal behavior are calculated using Equations (4) and (5), where $\bar{x}$ is the mean value, σ is the standard deviation and α is a sensibility level.

$$UCL = \bar{x} + \alpha\sigma \tag{4}$$

$$UCL = \bar{x} - \alpha\sigma \tag{5}$$

For normal control limits, we assume α=3 [24]. However, we can establish warning upper and lower limits (WUL and WLL, respectively) at *α=2*. Figure 3 shows the control chart for the normal behavior of sensors using the Euclidean distance.

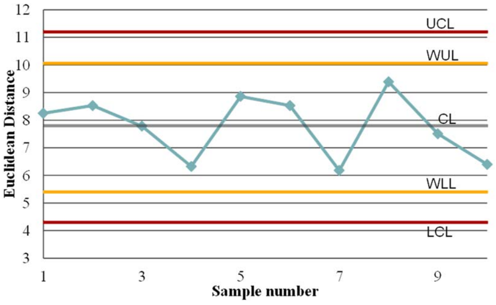

Fig. 3. Control chart for normal behavior (temperature sensor)

D. Classification

Once the ABA module has determined that there is an abnormality in the data provided by the sensor, the classification unit function is to identify the type of observed abnormality. For this task the Euclidean distance is used to detect behaviors and trends. For example in a DoS attack, the distance shows sudden changes above the UCL.

E. Recovery actions

When an abnormal behavior is detected, several recovery actions can be taken (e.g. discard data, authenticate the sensor, change network configuration, etc.). However, there is a possibility that the attack cannot be classified (e.g. new attacks), in such cases the data is rejected.

V. Experiments and Results

There are two phases to implement the ABA methodology, in both phases we use eight levels of decomposition for DWT; that means that the sensor behavior is inspected every 256 samples. Sensor's samples are taken every 10 ms because the ABA system needs around 3 seconds to detect and classify an abnormality. All the experiments were conducted in the SHT environment. In what follows we describe the experiments and the obtained results for each phase.

A. *Offline Training Phase*

The first step in the offline training phase is to build the matrix for sensor's classification. This is also part of the reference model since the runtime data will be compared with the elements contained in the matrix. Table 2 summarizes the mean value and the limits of normal operation (as explained in section IV-C) for the different sensors that are used in our experimental evaluation.

TABLE II. Normal Operation Limits

Sensor	Mean	UCL	LCL
Temperature	7.80	11.2	4.3
Motion	3161.08	5238.43	1083.73
Distance	14.54	18.20	10.78
Moisture	4.54	7.00	2.07
Power	32.05	35.55	28.55
Illumination	6.60	8.67	4.53

Once the system has been trained for the normal behavior of a given sensor, the next step is to launch attacks against that sensor to learn its behavior under attacks. The classification of the attacks is based on the trend of the Euclidean distance (see Figure 4).

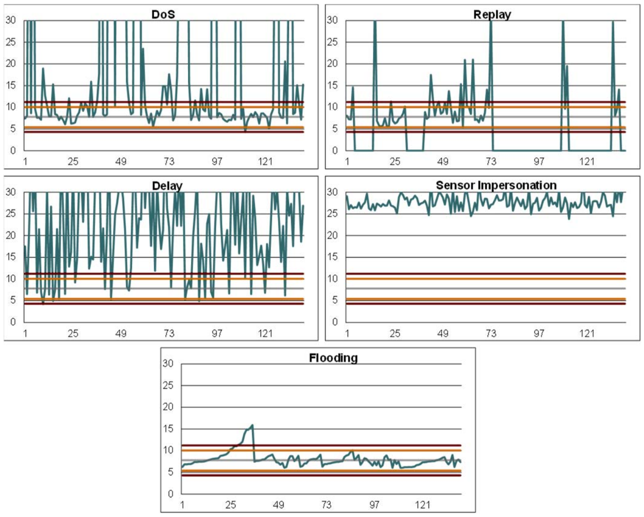

Fig. 4. Sensor behavior under attacks.

Depending on the intensity of the attack, it is possible to detect it before it goes out of the control limits by applying the trend rule. This rule applies also for unknown attacks since the Euclidean distance is developed for the normal distribution. A window of seven continuous Euclidean distances is used to verify any trend in the behavior. However, for some attacks (e.g. DoS), the seven samples are not needed since the Euclidean distance goes out of the control limits rapidly.

B. *Online Testing phase*

Once the s-DNA profile is obtained during the offline training phase, the system is tested and evaluated for a wide range of cyberattacks. Figure 5 shows the comparison between normal and abnormal behavior of a temperature sensor under DoS attack. Notice that some values are above the UCL for the abnormal behavior while other values are in the normal behavior area. This happens because the attacks were performed several times during the experiment. In Figure 5, one sample is a Euclidean distance, meaning that, each point in the graph needs 256 sensor readings.

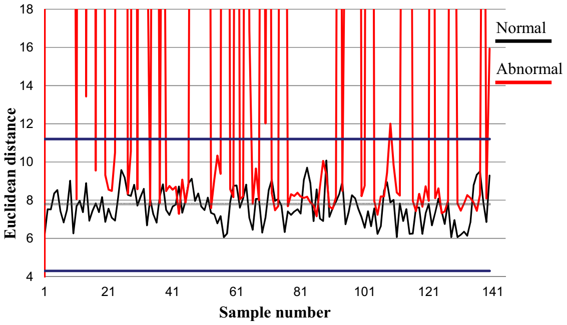

Fig. 5. Normal Behavior vs Abnormal Behavior (DoS).

We have evaluated the performance of our ABA approach for the attacks shown in table 3 when they are launched against all the sensors available in our testbed. It also summarizes the detection and classification accuracy of our approach for each attack type.

TABLE III. Tested attacks

Attack	Detection Rate	Classification Rate
Replay Attack	95 %	98 %
Delay Attack	96 %	88 %
DoS Attack	98 %	98 %
Flooding Attack	95 %	98 %
Sensor Impersonation	98 %	85 %
Pulse DoS	98 %	90 %
Noise injection	95 %	95%

From Table III, the pulse DoS and noise injection attacks are two new attacks that were not used during the offline training phase. Here the system detects these attacks and classify them as "new attack". There are two cases that trigger false positives, the first case happens when the behavior is not considered in the training phase (e.g. a cold object near the temperature sensor). In the second case, the sensor needs to reach its steady state after an attack. Our experiments show that at most 4.2% of these situations produced false positives alerts. Once the attack is detected and classified, the needed actions to solve the problem are taken. The actions include: 1) reject sensor's data, 2) launch an alert, and 3) deauthenticate the sensor. All the data contained in the sample is discarded and the sensor is asked to resend the data again so it can be authenticated by using its s-DNA (sensor discovery).

Table IV shows that our ABA-IDS has a detection rate better than the compared approaches for unknown attacks and, unlike signature-based IDS, it is able to detect new attacks.

TABLE IV. DETECTION RATE COMPARISON

Attack	Detection Rate (Kown Attacks)	Detection Rate (Unknown Attacks)
Specification IDS [25]	98%	80%
Signature IDS [26]	100%	0%
Secure HAN [27]	100%	60%
Our ABA-IDS	98%	95%

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we presented an IoT security framework for smart infrastructures that consists of four layers: devices (end nodes), Network, Service and Application layers. We also presented a methodology to develop a threat model that can be used to identify potential attacks against each layer, their impacts and how to mitigate and recover from these attacks. In our experimental results, we showed how to use the threat model to secure and protect sensors in smart IoT infrastructure. Our anomaly behavior analysis methodology includes the use of a sensor-DNA profile (s-DNA) that is developed to accurately characterize normal sensor operations. We have also shown that the ABA approach can detect both known and unknown attacks with high detection rates and low false positive alarms (around 4.2%). We have also developed an attack classification methodology with a 98% accuracy for known attacks and up to 95% for unknown attacks (classified as "new attacks"). We are currently extending our ABA methodology to the other layers of the IoT security framework.

ACKNOWLEDGMENT

This work is partly supported by the Air Force Office of Scientific Research (AFOSR) Dynamic Data-Driven Application Systems (DDDAS) award number FA95550-12-1-0241; National Science Foundation research projects NSF IIP-0758579, SES-1314631, and DUE-1303362, Thomson Reuters in the framework of the Partner University Fund (PUF) project (PUF is a program of the French Embassy in the United States and the FACE Foundation and is supported by American donors and the French government); National Instruments though its NI Research Academic Grant 2015.

REFERENCES

[1] Verizon (January, 2015). Create intelligent, more meaningful business connections. Retrieved from http://www.verizonenterprise.com/solutions/connected-machines/

[2] Z. Andrea, B. Nicola, Angelo C., Lorenzo V., and Michele Z., "Internet of Things for Smart Cities", IEEE Internet of Things journal, vol. 1, no. 1, February 2014.

[3] D. Kushner, "The Real Story of Stuxnet, How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 2013.

[4] A. Buckman, S. Myfield, M. Beck, "What is a Smart Building?", Smart and Sustainable Built Environment, Vol. 3, Issue 2, 2014.

[5] Z. Wang, L. Wang, A. Dounis, R. Yang, "Multi-agent control system with information fusion based comfort model for smart buildings" Applied Energy, Volume 99, pp. 247-254, 2012.

[6] M. Sadiku, S. Musa, O. Momoh, "Cloud Computing: Opportunities and Challenges", Potentials, IEEE (Volume: 33, Issue: 1), February 2014.

[7] Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. (April 2015). [Online] Available: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

[8] H. Suo, J. Wan, C. Zou, J. Liu, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, vol. 3.

[9] C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[10] S. Greengard, "Cybersecurity Gets Smart", Communications of ACM, May 2016, Vol. 58, No. 5, pp. 29-31

[11] O. Can, O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks", 6th IEEE International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.

[12] S. Fayssal, S. Hariri, Y. Al-Nashif, "Anomaly-Based Behavior Analysis of Wireless Network Security", Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2007.

[13] Scott Musman, Mike Tanner, Aaron Temin, Evan Elsaesser and Lewis Loren, "Computing the Impact of Cyber Attacks on Complex Missions", 2011 IEEE International Conference on Systems (SysCon).

[14] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska, and W. Xu, "Automated Security Test Generation with Formal Threat Models", IEEE transactions on dependable and secure computing, vol. 9, no. 4, July/August 2012.

[15] R. Schlegel, S. Obermeier, J. Schneider, "Structured System Threat Modeling and Mitigation Analysis for Industrial Automation Systems", IEEE 13th International Conference on Industrial Informatics (INDIN), July 2015.

[16] Eun-Kyu Lee, Peter Chu, and Rajit Gadh University of California, Los Angeles, "Fine-Grained Access to Smart Building Energy Resources".

[17] Jiong Jin, Jayavardhana Gubbi, Slaven Marusic, and Marimuthu Palaniswami, "An Information Framework for Creating a Smart City Through Internet of Things"

[18] Hiro Gabriel Cerqueira Ferreira, Edna Dias Canedo, Rafael Timóteo de Sousa Junior, "IoT Architecture to Enable Intercommunication Through REST API and UPnP Using IP, ZigBee and Arduino"

[19] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou1, C.Lung, "Smart Home: Integrating Internet of Things with Web Services and Cloud Computing", IEEE 5th International Conference on Cloud Computing Technology and Science, 2013.

[20] P.K. Manadhata, J. M. Wing, "An Attack Surface Metric", IEEE Transactions on Software Engineering, vol. 37, no. 3, May/June 2011.

[21] M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services.

[22] A. Kozionov, M. Kalinkin, A. Natekin, A. Loginov, "Wavelet-Based Sensor Validation: Differentiating Abrupt Sensor Faults From System Dynamics", IEEE 7th International Symposium on Intelligent Signal Processing (WISP), 2011.

[23] S. Mallat, "A Wavelet Tour of Signal Processing, Third Edition: The Sparse Way", 3rd Edition, Elsevier, ISBN-13: 978-0123743701

[24] D. C. Montgomery, "Statistical Quality Control", 7th Edition, John Willey & sons, ISBN-10: 1118146816.

[25] P. Jokar, H. Nicanfar, V. Leung, "Specification-based Intrusion Detection for home area networks in smart grids," IEEE International Conference on Smart Grid Communications , pp.208-213, Oct. 2011

[26] B. Al-Baalbaki, J. Pacheco, C. Tunc, S. Hariri, Y. Al-Nashif, "Anomaly Behavior Analysis System for ZigBee in smart buildings", IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Morocco, 2015.

[27] V. Namboodiri, V. Aravinthan, S. Mohapatra, B. Karimi, W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," IEEE Systems Journal, no.99, pp.1-12.