A Cognitive Framework to Secure Smart Cities

Shahab Tayeb[1], Neha Raste[1], *Matin* Pirouz[2], and *Shahram* Latifi[1]

[1]Department of Electrical and Computer Engineering, University of Nevada, Las Vegas, USA
[2]Department of Computer Science, University of Nevada, Las Vegas, USA

Abstract. The advancement in technology has transformed Cyber Physical Systems and their interface with IoT into a more sophisticated and challenging paradigm. As a result, vulnerabilities and potential attacks manifest themselves considerably more than before, forcing researchers to rethink the conventional strategies that are currently in place to secure such physical systems. This manuscript studies the complex interweaving of sensor networks and physical systems and suggests a foundational innovation in the field. In sharp contrast with the existing IDS and IPS solutions, in this paper, a preventive and proactive method is employed to stay ahead of attacks by constantly monitoring network data patterns and identifying threats that are imminent. Here, by capitalizing on the significant progress in processing power (e.g. petascale computing) and storage capacity of computer systems, we propose a deep learning approach to predict and identify various security breaches that are about to occur. The learning process takes place by collecting a large number of files of different types and running tests on them to classify them as benign or malicious. The prediction model obtained as such can then be used to identify attacks. Our project articulates a new framework for interactions between physical systems and sensor networks, where malicious packets are repeatedly learned over time while the system continually operates with respect to imperfect security mechanisms.

1 Introduction

The world is at the brink of a new digital revolution and Cyber Physical Systems (CPS) based on the Internet of Things (IoT) networks mark the next frontier. IoT allows companies to increase productivity, city services to converge, vehicles to become autonomous, and homes to become smarter. There has been much research on the design, evaluation, testing, and verification of CPS and its associated IoT. Nonetheless, research on the development of security models and frameworks for IoT networks is very limited. A key challenge is that security solutions for IoT should not hinder the openness of the network, nor should they introduce additional latency or overhead to communications across the network. These requirements are achieved by incorporating security into the design of IoT infrastructures. This project is focused on two main principles: “adaptive security architecture” and “IoT-based CPS or ICPS” both of which are listed on Gartner’s 2016 top 10 strategic technology trends.

Dozens of hardware platforms of embedded systems are gaining popularity as prototypes of IoT [1-2]. Smart objects and embedded sensors are currently secured based on the same best practices of traditional networks without considering the limitations imposed by the proliferation of smart nodes in terms of processing power and memory. This is mainly due to limited research in this field. Encapsulation of protocol stack layers is done on a single hardware processor and thus, leaving the lower layers unprotected has detrimental effects. With so many new forms of data, new forms of threats will come to existence targeting them.

Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) can be found as standalone platforms, or as modules integrated into other hardware, or even as software applications with the two categories of IDS being Network-based and Host-based IDS. New generations of devices bring along newer and more sophisticated generation of threat agents and attacks. This concern is addressed by integrating security in design and thus, preventing the problem from happening. ICPS lack a secure design for implementation. Because IoT systems utilize diverse protocols and technologies encompassing a wide array of technology concepts such as Application Programming Interfaces (APIs), sensor-equipped edge devices, and messaging protocols, they are prone to different attacks. Additionally, lack of standardization to support IoT increases heterogeneity of these networks and introduces inoperable components which will create vulnerabilities. Because of utilizing a wide array of heterogeneous and often unreliable smart objects, there is a need for a reliable design model capable of supporting bandwidth-intensive applications.

The design objectives of this framework are twofold: first, to address security concerns; and second, to provide on-demand security guidelines for the next generation of CPS. The research questions are: a) What are the security vulnerabilities and challenges presented by the emerging technologies (e.g. 802.11.5, ZigBee, GPRS,

LTE) in providing IoT connectivity? b) Can Deep Learning (DL) be as successful on IoT security as it has been in computer vision and speech recognition? c) Can security by design guideline and frameworks outperform the existing security patches and protocols? and d) How different are the security gaps for smart city sensors and gateways from those of traditional networks.

2 Vulnerability analyses

2.1. IoT Security

The IoT is composed of many layers of technologies, each with its own set of security challenges. Smart devices are more capable of gathering and curating sensed data which makes them more susceptible to being targeted by a variety of attack types from single target impersonation, rogue nodes, and privileged access to batched ones such as botnets and DDoS. It has been reported by FCC's Technological Advisory Council (TAC) that hackers have the lead in breaching the IoT security. The reasons are threefold: i) Conventional network security wisdom is not applicable to the IoT realm. IoT is an ecosystem driven by business gaps, rather than just a myriad of devices; ii) IoT manufacturers don't prioritize security and lack a security culture. IoT vendors compromise security to gain functionality and openness for a broader target market. IoT manufacturers follow agile manifesto for their development process which opens up many security gaps; and iii) There are inherent vulnerabilities in individual IoT nodes: a) For many types of IoT devices, physical access cannot be restricted, thus devices that expose critical information on internal nodes can be compromised; b) Although chip manufacturing innovations have led to the emergence of embedded chips with hardware-based security (e.g. ARM TrustZone) and hardware with cryptography support (e.g. ARMv8), the inclusion of such chips in every device is cost prohibitive. Thus, it makes sense to look for network security solutions that do not require modification of existing and emerging IoT devices; and c) IoT nodes generally don't support advanced networking capabilities and in particular security protocols. The proposal aims to advance insight to IoT and identify its vulnerabilities, while attempting to develop methodologies to guard against cyber-attacks that can penetrate the IoT layers through a wide range of heterogeneous devices. Securing systems from a network design perspective defines security zones and layers based on data requirements of each network segment, independently of device type and location. This is different from encrypted IoT chips and restricted physical access to IoT nodes, and enhances protection against zero-day attacks and well-known threats.

2.2 Smart City

Cities are rapidly converging toward digital technologies to provide advanced information services, efficient management, and resource utilization that will positively impact all aspects of our life and economy. This has led to the proliferation of ubiquitous connectivity to critical infrastructures (electrical grid, utility networks, health care, finance, etc.) that are used to deliver advanced information services to homes, businesses, and government. On the other hand, such smart systems are more complex, dynamic, heterogeneous, and have many vulnerabilities that can be exploited by cyberattacks. Protecting and securing the resources and services of smart cities become critically important due to the disruptive or even potentially life-threatening nature of a failure or attack on smart cities' infrastructures.

A resilient architecture that protects smart cities' communications, controls, and computations based on autonomic computing and Moving Target Defense (MTD) techniques was proposed in [3]. The key idea was to make it extremely difficult for the attackers to figure out the current active execution environments used to run smart city services by randomizing the use of these resources at runtime.

An important part of Smart City is wireless communication networks which are pervading the IoT realm due to their fast, easy, and inexpensive deployment. Pervasive wireless technologies have higher security requirements. Even though the existing security protocols for wireless communications address the privacy and confidentiality issues, various unaddressed vulnerabilities exist. Such vulnerabilities target cyber and physical availability of the systems, spoof data link and network layer addresses protocols, or even upper layer session hijacking.

Table 1. Mapping known attacks to smart city

Attacks	Main Characteristics	Mapping to Smart City
DoS	Rendering a device unusable through exhaustion of target's resources	Smart City sensors/loggers have more limited resources (e.g. CPU & RAM)
DDoS	A type of DoS where the source are thousands of zombies	50 billion devices targeted to become zombies and the same 50 billion are potential victims
IP Spoofing	An unauthorized use of someone else's logical address	More valid addresses increase susceptibility of spoofing attacks
Physical Attack	Someone getting physically close to network components	More connected devices equal easier physical access to them
Eaves-dropping	Type of reconnaissance	More data leads to a higher probability of reconnaissance gaps
Sybil	Subversion of reputation systems by forged identities in peer-to-peer networks	Wireless Sensor Networks are the main target for Sybil attacks
Black hole	Packet drop on intermediary devices	Limited resources on Smart City sensors and nodes are easy targets

2.3 Smart city data analytics

Smart city can be illustrated as a complex network with different types of relationships. These relationships can be as simple as a one direction data connection to as complicated as a weighted prioritized two-way connection between a gateway and a data logger. Smart nodes are placed in communities of similar purpose devices. Based on the Confidentiality, Integrity, Security (CIA) mechanisms and addressing such vertices using Authentication, Authorization, Accounting (AAA), smart city security is adding different layers of access for every user of the network. Finding communities of similar devices with similar purposes is possible through evaluating similar relationship between devices which are known as nodes in the networks. Finding these communities can help level out and separate different levels of domains for various type of relationships and access.

In today's world, networks are as big as billions of nodes and smart cities are no different. To secure them, we need to put them in partitions and secure each partition both separately and as a group. To find these partition, also known as communities, there are big data community detection algorithms that could be used. Also ranking the partition could facilitate finding out which partitions can achieve a higher level of security. Security can be better handled if appropriate set of partitions are identified within the networks. With sub-partitioning, systems such as Hadoop can make the parallel data handling possible [4].

2.4 Existing methods

Alipour et al. [5] analyzed intrusion detection systems for Media Access Control (MAC) and Physical Layer (PHY) specifications using an anomaly-based behavioral analysis to detect abnormal behaviors, which are likely to be triggered by threat agents. They did this by monitoring the n-consecutive transitions of the protocol state machine. Then, sequential Machine Learning techniques were applied to model the n-transition patterns in the protocol. The probabilities of these transitions were normalized, reaching a low false positive of less than 0.1%. Spoofers impersonate legitimate users to exploit the user services and privileges. The Semi-Global Alignment algorithm (SGA) is an efficient technique to detect spoof attacks. The limitation of SGA is that it cannot be applied to large scale, multiuser systems due to high false positive rates.
Kholidy et al. [6] proposed the Data-Driven SGA which improves the scoring systems using distinct alignment parameters per user. It also adapts to changes in the user behavior by updating the signature of a user according to his/her current behavior. The main objective of this proposal is to design a secure architectural framework for implementation of IoT-based, small to large-scale CPS in Smart City. This is important because of the inevitable migration to IoT networks and the unsafe and insecure nature of the underlying sensor-embedded smart objects, which interact with the physical world. Traditional security solutions might address security needs of IoT in part but there are challenges such as platform security limitations, ubiquitous mobility, mass quantities, and cloud-based operations that are not addressed.

3 The proposed approach

This research proposes a tunable underlying framework for IoT networks of different sizes which will, in turn, open many new research opportunities in IoT security. In addition, this research will facilitate and expedite adoption of small to large-scale IoT-based. But in the CPS context, security takes new forms and some of the previously used solutions such as Host-based IDS are not practical due to limited hardware resources on endpoint sensors. Adding to the issue is the fast-growing number of such sensors and their faster adoption by the public resulting in their widespread use without taking into account the many security gaps. Together with scientific advances in sensing and communications technologies, many consumers are using body sensors, connecting their generated data to their online profiles, or storing them on their smartphones or laptops. This project employs four technologies or methods as discussed below. The logical relation among these pieces is presented in Figure 1.

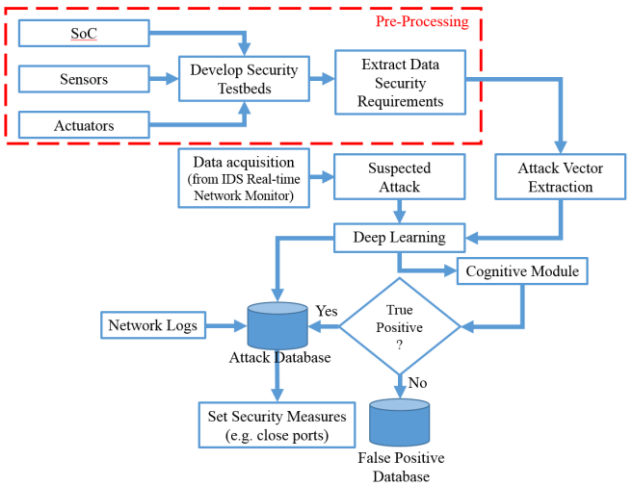

Fig. 1. Framework-Development Process

Anomaly-based, also called behavior-based, methods assume that attackers behave differently than normal users. The advantage of this method is the ability to spot a threat without first knowing its signature. Historically, this advantage has been offset by high false positive rates, the difficulty of training a system in a highly dynamic environment, and computational expense [7]. Some instances of the targeted vulnerabilities are presented in Table 2. It should be noted that most of the new attacks are typically minor mutations of the known ones, which leads us to believe that the DL approach can be successful on detecting imminent attacks. DL methods are successfully incorporated in various domains because DL relies on local proximity (typically spatial and/or temporal) among patterns to find and construct higher order patterns (Figure 2).

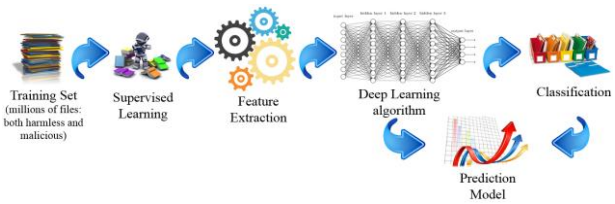

Fig. 2. Overarching Scheme of Threat Prediction

The factors moving Machine Learning tools and techniques from the research lab to the operational domain include both the phenomenal growth in inexpensive compute power and bandwidth and the overwhelming amount of data generated and dumped into Security Information and Event Management (SIEM) tools daily. Although Machine Learning tools can be very effective, they produce very different results depending on the source and quality of data being analyzed. Specific domain knowledge related to security—as opposed to clinical research or finance, for example—is needed to design a threat detection system using appropriate Machine Learning mathematical and statistical algorithms. A data scientist must apply security domain knowledge to identify primary and secondary sources of data, determine how to clean and transform acquired data and select the best Machine Learning analytical method or algorithm for the problem at hand. Primary sources for the security domain include network packets, Machine Learning -based analysis of which reveals otherwise invisible communication patterns from an attacker inside the network. Secondary sources are logs routinely collected from other devices, which may provide additional depth to the analysis but not direct evidence of activity due to the nature of logs' role in providing security defences [7].

4 Results and discussions

DL [13] is a field that encompasses machine learning so it can be used to learn intricate patterns from large volumes of data. It is generally an architecture formed out of neural network activation functions. Supervised and Unsupervised learning refer to labeled and non-labeled data respectively [14]. For supervised learning, techniques such as Recurrent Neural Networks (fast and efficient), Convolutional Neural Networks (Time consuming, but suitable for special data, such as images), Long Short Term Memory (which can be used for vanishing gradient problem [15] which occurs nearing the end of training, where gradient is supposed to be really less) apart from the traditional neural networks such as Deep Boltzmann Machines or Deep Belief Networks as well as fully connected, slow-to-train Multi-Layer Perceptron [14]. Each layer of the deep models shown below can be consisting of linear or complex activation functions depending on the overall complexity of the problem. For instance, for malware detection problem, we stacked two layers with linear activations with two layers of Rectified Linear Units in between them. This was implemented to get the best accuracy of prediction for the given data [16]. In this study, CSIC 2010 HTTP Dataset was used to detect web attacks using session IDs and indices. This data set has been widely used for abnormal behavior detection. Regarding web traffic, some of the problems of this data set are that it is out of date and also that it does not include enough actual attacks and hence, it is criticized by security researchers.

This is a proven benchmark initially set for researchers to compare different methods of detection and classification of network attacks. It was built as an improvement over the earlier KDD Cup 1999 dataset in the form of a reduction in redundant records, proportionate number of records in each difficulty level group [16]. Experts believe that new attacks can be mostly identified by the signature of the known attacks. According to this principle, we train the data on the features given in this dataset, and some derived from them. They include, but are not limited to the duration, protocol type, destination network service, source and destination lengths in bytes, flags, number of wrong fragments, the number of high QoS packets, etc. The results show the logistic regression classification, where the Dependent Variable is categorical, can perform anomaly detection efficiently. The ROC curve characterizing the preliminary results is outlined in Figure 3. As illustrated in Figure 3, a simple logistic regression classification with two parameters can achieve a performance of 64%. Utilizing DL techniques with a multitude of features results in higher accuracy. Logistic regression classifies data into two categories, and the Receiver operating characteristics (ROC) curve indicates the area under the curve which signifies the percentage of accurate classification. According to the results on the dataset, accuracy percentage is 86%. A standard metric to evaluate logistic regression classification is accuracy, which is calculated by dividing true Positives over the sum of false positives and true positives.

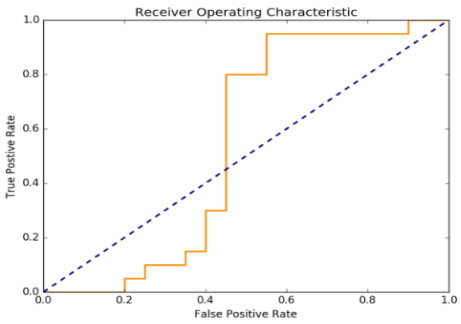

Fig. 3. ROC Curve of Logistic Regression

The learning model consists of an input vector X. Logits are outputs of linear functions – that are continuous and differentiable. Logits need to be converted into a scale of probabilities [0,1]. The weight and bias parameters need training. This linear block can be cascaded with multiple different linear blocks that sum up to learn different features of the input. However, to increase the complexity to define finer features of the input, we need a combination of non-linear elements that can do so. This can be achieved by combining rectified linear units that scale inputs. Once Softmax function

converts logits into probabilities we can use these values to be given to series of Rectified Linear Units.

Rectified Linear Units (ReLUs) can be shown as:

$$f(x) = \sum_{i=1}^{inf} \sigma(x - i + 0.5) \approx \log(1 + e^{x})$$

where, x = input vector, f(x) = output of a rectified linear unit. A series of ReLUs [17] cascaded together can form a computationally expensive, although fairly efficient non-linear differentiable model to model complexities of a function. ReLUs can be replaced by functions such as Sigmoid, Tanh, etc. Figure 4 presents the comparison diagram of such non-linear functions for the preliminary results. Sigmoid functions are used for logistic regression functions. ReLUs outperform sigmoid and give better classification accuracy only by a slight margin. Thus, both are widely used and give comparable results. They introduce non-linearity while pooling up layers of one convolutional layer on others. Components of the learning model are depicted in Figure 5.

In general, the linear blocks or layers can be stacked upon each other, with non-linear interface as shown below. DL Model (forward propagation) [18] is the very basis of learning in which features from the first layer is carried forward to the next layer. For training, a widely popular algorithm is Back-Propagation [19], in which gradients or relative difference between iterations of calculating weight functions are minimized by a backward-looking architecture as shown below. Back propagation is a mean-squared-error function which is differentiable.

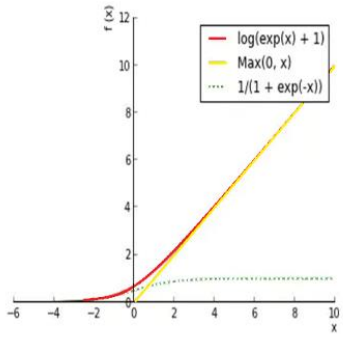

Fig. 4. ReLUs and Max-Pooling/Sigmoid Functions

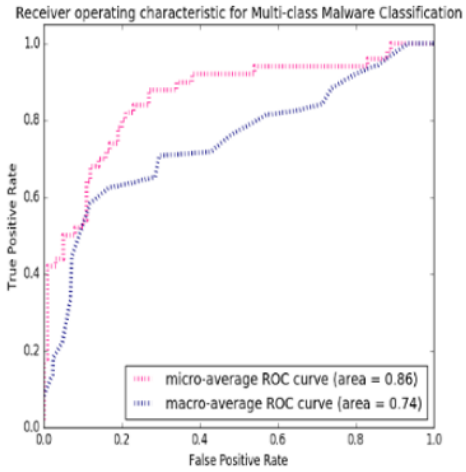

Fig. 4. Classification Results

This work is supported in part by the Doctoral Graduate Research Assistantship from UNLV Graduate College and in part by the NSF award #EPS-IIA-1301726 (EPSCoR NEXUS).

References

1. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M., "Security and privacy challenges in industrial Internet of Things," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, pp.1-6, 8-12, June 2015.
2. S. Tayeb, S. Latifi and Y. Kim, "A survey on IoT communication and computation frameworks: An industrial perspective," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6. doi: 10.1109/CCWC.2017.7868354
3. J. Pacheco, C. Tunc and S. Hariri, "Design and evaluation of resilient infrastructures systems for smart cities," 2016 IEEE International Smart Cities Conference (ISC2), Trento, 2016, pp. 1-6. doi: 10.1109/ISC2.2016.7580756
4. Pirouz, Matin, Justin Zhan, and Shahab Tayeb. "An optimized approach for community detection and ranking." Journal of Big Data 3.1 (2016): 22.
5. H. Alipour, Y. B. Al-Nashif, P. Satam and S. Hariri, "Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2158-2170, Oct. 2015. doi: 10.1109/TIFS.2015.2433898
6. H. A. Kholidy, F. Baiardi and S. Hariri, "DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 2, pp. 164-178, March-April 1 2015. doi: 10.1109/TDSC.2014.2327966
7. Barbara Filkins, "the Expanding Role of Data Analytics in Threat Detection", SANS Whitepaper, October 2015.
8. Farooq MU, Waseem M, Khairi A, Mazhar S. A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications. 2015 Jan 1;111(7).
9. Kolias C, Stavrou A, Voas J, Bojanova I, Kuhn R. Learning Internet-of-Things Security" Hands-On". IEEE Security & Privacy. 2016 Jan;14(1):37-46.
10. S. Ray, S. Bhunia, Y. Jin and M. Tehranipoor, "Security validation in IoT space," 2016 IEEE 34th VLSI Test Symposium (VTS), Las Vegas, NV, 2016, pp. 1-1. doi: 10.1109/VTS.2016.7477288
11. R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 336-341. doi: 10.1109/ICITST.2015.7412116
12. S. A. Zonouz, R. Berthier, H. Khurana, W. H. Sanders and T. Yardley, "Seclius: An Information

Flow-Based, Consequence-Centric Security Metric," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 562-573, Feb. 2015. doi: 10.1109/TPDS.2013.162

13. G. E. Dahl, J. W. Stokes, L. Deng and D. Yu, "Large-scale malware classification using random projections and neural networks," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 3422-3426
14. Salakhutdinov, Ruslan, and Geoffrey E. Hinton. "Deep Boltzmann Machines." AISTATS. vol. 1. 2009.
15. S. Yuan, X. Wu and Y. Xiang, "Incorporating Pre-Training in Long Short-Term Memory Networks for Tweets Classification," 2016 IEEE 16th International Conference on Data Mining (ICDM), Barcelona, Spain, 2016, pp. 1329-1334
16. Dataset for KDD Cup and Workshop, ACM SIGKDD, San Jose, California, Aug 12, 2007. James Bennett, Charles Elkan, Bing Liu, Padhraic Smyth, and Domonkos Tikk. 2007. KDD Cup and workshop 2007. SIGKDD Explor. Newsl. 9, 2 (December 2007), 51-52. doi: 10.1145/1345448.1345459
17. Nair, Vinod, and Geoffrey E. Hinton. "Rectified linear units improve restricted boltzmann machines." Proceedings of the 27th international conference on machine learning (ICML-10). 2010.
18. R. Sánchez, A. Arpi and L. Minchala, "Fault Identification and Classification of Spur Gearbox with Feed Forward Back Propagation Artificial Neural Network," 2012 VI Andean Region International Conference, Cuenca, 2012, pp. 215-215.
19. Y. Liu, W. Jing and L. Xu, "Cascading model based back propagation neural network in enabling precise classification," 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Changsha, 2016, pp. 7-11