Detection and Classification of Attacks on IoT Networks

Completed Research

Agnieszka Onuchowska
University of South Florida
aonuchowska@mail.usf.edu
Wolfgang Jank
University of South Florida
wjank@usf.edu

Saurav Chakraborty
University of South Florida
sauravc@mail.usf.edu
Utkarsh Shrivastava
Western Michigan University
utkarsh.shrivastava@wmich.edu

Abstract

In this article we are analyzing how Industrial Internet of Things (IIoT) sensors and devices behave while they undergo an attack. Using data generated from a controlled experiment where attacks were carried out on a Secure Water Treatment (SWaT) system, we analyze the behavior of the sensors. We observe that the readings from the sensors are non-linear in nature and resemble ECG waveform output, which helps in identifying inconsistencies or anomalies in heartbeats of patients. Through the comparison of sensor behavior during an attack and under normal conditions we find a significant difference in the features of the waveforms. Also, we look at the contrasting behavior of sensors under two different kinds of attacks: physical and cyber. The findings of this research motivate an alternative approach for anomaly detection and real time assessment of cyber-attacks on IoT devices with the use of analytics.

Keywords

IoT Networks, Cybersecurity, Attack Topology, Anomaly Detection

Introduction and Motivation

Smart city solutions that rely on interconnected Industrial Internet of Things (IIoT) sensors and devices have gained wide interest over the recent years because of their contribution to the quality of services provided to citizens (Kitchin & Dodge, 2017, Thibodeaux, 2017). For example, real-time data collected over smart water management systems can measure water quality or detect leaks (Cerrudo, 2015) and sensors that collect information about the movement of people and vehicles help to streamline city traffic flows (Maddox, 2016). The number of smart devices deployed in transportation services, hospitals, power plants or water management facilities has been intensively increasing over the past years (Sleptchenko & Johnson, 2015). Connected things in smart cities reached 2.3 billion devices in 2017 (Thibodeaux, 2017) and the number is expected to expand to 50 billion devices by 2022 (Elfrink, 2012). Implementation of smart technologies brings tangible cost savings to cities. For example, Barcelona has been saving $58 million/ year after the city installed smart water-meter technology (Horwitz, n.d.). Nevertheless, smart systems are often exposed to vulnerabilities, the consequences of which are not yet fully understood (Kitchin & Dodge, 2017, Ransbotham et al. 2016). As critical city infrastructure is increasingly dependent on smart devices, it has also become a target of cyberterrorist or hacker attacks (Oliveira, 2010, Sleptchenko & Johnson, 2015).

IIoT-based devices are listed as one of the top four future IS-related challenges, which are likely to cause significant problems and generate multiple adverse implications (Ransbotham et al., 2016). Examples of intentional disruption can take the form of malware attacks on container ports and cyber-attacks on water dams (Sanger, 2016) as well as hacking attempts on pumping stations (Walter, 2017), tram infrastructure systems (Shukla, 2017), power grids (Sanger, 2016) or emergency warning systems (Rosenberg & Salam, 2017). Attacks on city infrastructure can result in blackouts (Sanger, 2016), improper functioning of city traffic light systems (Jones, 2016) or disrupted water supply and wastewater treatment (Walton, 2017). Examples of past attacks on water management systems include attacks on water pumps (Nakashima, 2011) or valves that control the flow of chemicals (Leyden, 2016). The lack of physical controls that monitor IIoT-supported devices has already been causing security failures. More security shortcomings resulting in biological or chemical water contamination as well as physical disruption of water treatment plant infrastructures are likely to follow (Sleptchenko & Johnson, 2015, Ransbotham et al., 2016, Espelund, 2016). Our motivation for this study is backed by the fact that the number of cyber-attacks on IIoT-supported water treatment plants has recently been increasing (Walton, 2016), whereas cybersecurity controls, which would help to detect such cyber-attacks, are usually not in place (Speake, 2015).

Secure management of an interconnected network of IoT devices is based on two types of defense mechanisms: the detection-based method, such as intrusion detection (further divided into misuse detection and anomaly detection) as well as a prevention-based approach such as access control (Wu et al., 2016, Wang et al., 2004). The anomaly-detection approach is effective against new types of security attacks as it models normal system behavior as a baseline. Consequently, such an approach not only helps to identify already known types of attacks but also effectively spots new types of attacks (Wang et al., 2004, Patcha & Park, 2007) and could be deployed in identifying new types of IoT network anomalies and attacks. In this paper we propose a statistical anomaly-based detection of water treatment system cyber-attacks. We analyze data on water quality collected over a lab-controlled series of attacks and compare the data against normal operation of the water system. In order to better analyze the problem of anomaly patterns, we refer to electrocardiographic (ECG) waveform analysis (Horowitz, 1975, Wang et al., 1989, Ono et al., 2004, DeMarzo & Lang, 1996) and draw similarities between graphical output of water quality monitoring patterns and an ECG signal. Given the spiky and non-linear nature of the water monitoring sensor data, traditional methods of curve-fitting will not be applicable. Past research in aberration of ECG waveforms could provide a good platform to analyze the water monitoring sensor readings. Hence, the research on ECG waveforms provides a good basis for the methodology of our study. In this research we are using cardiography waveform patterns and map past research methods with IoT network anomaly detection. Similarly to water quality pattern that changes over time, a heartbeat waveform has a non-periodic character (Wang et al., 1989). We hypothesize that similar to the flow of blood through the thorax, of which impedance changes can be captured by ECG (Packer et al., 2006), security attacks on water management systems can be identified with the use of statistic-based analysis of the waveforms produced by water quality sensors.

Related Work

Network Anomaly Detection

Numerous network anomaly detection methods that provide information about possible cyber-attacks have been developed in recent years. Fan et al. (2004) propose a distribution-based anomaly generation algorithm that is used to create anomaly detection models, which capture known and unknown intrusions. Hansen et al. (2007) use a genetic programming algorithm to detect system intrusions. Kim et al. (2017) propose a network anomaly detection technique based on grid partitioning approximation that is applied to analyze a given network dimension. Babaie et al. (2014) apply the Linear Dynamical System (LDS) to detect deviations from temporal and spatial correlations in the data, which ultimately leads to detection of a range of cyber-attack types. Jiang and Papavassiliou (2004) analyze normal network behavior patterns and propose an anomaly-tolerant traffic prediction algorithm that detects network attacks using the analysis of abnormal behavior generated in the network. Researchers propose that normal behavior patterns and profiles need to be identified so that potential future deviations could be then observed. Thottan and Ji (1999) apply an algorithm which uses sequential Generalized Likelihood Ratio (GLR) tests to identify faulty network performance. Bivens et al. (2002) propose neural network deployment with the use of supervised and unsupervised learning to analyze network traffic and detect possible network attacks. In turn, Tian and Ding (2014) use dynamic threshold base detection methods and apply diffusion wavelets to the analysis of anomalies in network traffic. Dominic and Said (2014) use outlier detection scheme in frequent pattern mining to distinguish anomalies in network traffic from normal network behavior. Our work offers extension of the previously used research methodologies by connecting existing approaches with cardiography methods used to detect heartbeat anomalies.

Pattern Detection in Cardiography

Cardiography waveforms are highly accurate and effective in monitoring normal heartbeat rates as well as identification of inconsistencies in patient heartbeats (DeMarzo & Lang, 1996). Waveforms that help to spot anomalies in heartbeat are based on precise measurements of peak amplitudes, durations of the significant peaks and shapes of waves (Horowitz, 1975). If simple averaging methods are employed directly to heartbeat signal waveforms, any distorted signals, caused by e.g., severe arrhythmias, can disrupt the original heartbeat signals and produce meaningless output (Wang et al., 1989). Filtering, smoothing or series approximation of heartbeat waveforms are not possible as when irrelevant peaks are removed, amplitudes and durations of significant peaks can be tampered (Horowitz, 1975).

Horowitz (1975) proposes approximation theory to encode a heartbeat waveform as a piecewise linear function. He also employs piecewise polynomial curve fitting (linear, quadratic or spline) as by this cardiography waveform approximation can follow without a change in its gross shape. An algorithm that is based on linear approximation and tabular parsing techniques is applied to capture peaks in cardiograph waveforms (Horowitz, 1975).

Data description

To analyze the problem of anomaly detection in a network of IoT devices, we investigate the water quality data collected over the lab-controlled series of attacks on a Secure Water Treatment (SWaT) system located in the Center for Research in Cyber Security at Singapore University of Technology and Design (Goh et al., 2016). The SWaT system is a scaled down version of an industrial water plant and is managed by SCADA workstation, a set of Programmable Logic Controllers and actuators as well as IoT sensors. The system is divided into six interconnected parts, each of which is responsible for subsequent water filtration activities. The system can produce up to five gallons of filtered water with the use of reverse osmosis and ultrafiltration techniques. This system consists of 54 IoT sensors, each of which collects the data from the environment on a second by second basis.

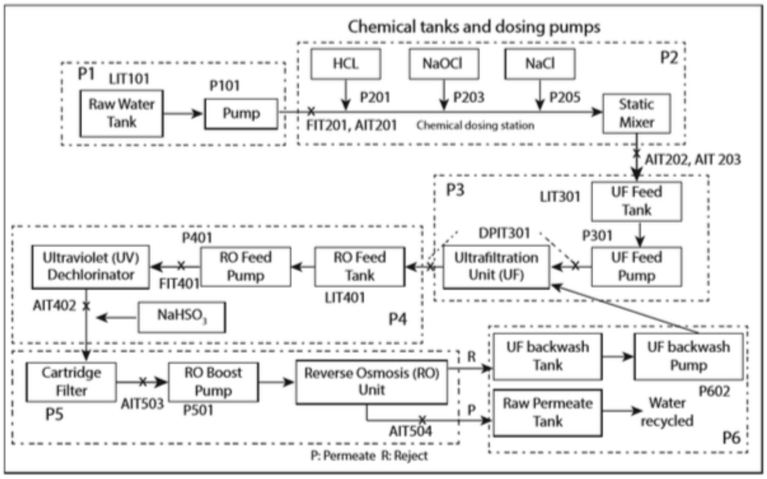

Figure 1: SWaT Testbed Process Overview (Goh et al., 2016)

Water quality analyzers

To measure water quality in the system, we select two sensors located in part 2 (P2), two sensors located in part 4 (P4) and four sensors located in part 5 (P5) of the water management system. The reason for selecting these analyzers is that since water is flowing in one direction from part 1 (P1) onwards to later parts, sensors located in more advanced parts of the system should experience impact from most attacks. The selected sensors of P2, P4 and P5, whose role is to monitor pre-defined water quality features, are as follows: pH level analyzer (AIT202, AIT501), water hardness analyzer (AIT401), sodium hypochlorite level analyzer (AIT402, AIT502) and sodium chloride level analyzer (AIT 201, AIT503 & AIT504).

Analyzer (Sensor)	Description	Range	Operating Range
AIT201	Conductivity analyzer; Measures NaCl level.	0-1000 µS/cm	30-260 µS/cm
AIT202	pH analyzer; Measures HCl level.	2-14	6-9
AIT401	Reverse Osmosis (RO) hardness meter of water.	0-150ppm	5-30ppm
AIT402	ORP meter; Controls the NaHSO3dosing, NaOCl dosing.	0-800mV	150-300mV
AIT501	RO pH analyzer; Measures HCl level.	2-14	6-9
AIT502	RO feed Oxidation-Reduction Potential(ORP) analyzer; Measures NaOCl level.	0-800mV	100-250mV
AIT503	RO feed conductivity analyzer; Measures NaCl level.	0-1000 µS/cm	200-300 µS/cm
AIT504	RO permeate conductivity analyzer; Measures NaCl level.	0-20 µS/cm	5-10 µS/cm

Table 1: Sensor functional descriptions (Goh et al., 2016)

Topology (classification) of attacks

A total set of 36 attacks on each of the 6 stages of the SWaT system were run during the attack experiment. The attacks were divided into 4 categories: (1) 26 Single Stage Single Point - attack on exactly one point in the Cyber Physical System (CPS), (2) 4 Single Stage Multi Point - attack on multiple attack points on one stage, (3) 2 Multi Stage Single Point - attack on single attack points on multiple stages, (4) 4 Multi Stage Multi Point - attack on multiple attack points that span through multiple stages.

Category of Attack	Number of Attacks
Single Stage Single Point	26
Single Stage Multi Point	4
Multi Stage Single Point	2
Multi Stage Multi Point	4

Table 2: Number of Attacks Per Category (Goh et al., 2016)

The dataset was collected over 11 days, out of which over the first 7 days the system was not attacked. During the remaining 4 days simulated cyber-attacks were induced. Each of the attacks lasted several minutes to one which lasted 10 hours. Conducted attacks were classified into two types: (1) manual attacks, where a sensor was physically manipulated, for example a pump was shut down or (2) cyber-attack, where the readings from analyzers were modified through the system, for example pH level of the water was reduced or sensor's reading was changed from high to low.

Problem Definition

IoT networks are greatly complex systems consisting of a high number of associated components (Ransbotham et al., 2016). Due to the high complexity of such networks, quick identification of anomalies in the system becomes difficult. Our goal is to identify if and when there is an anomaly in the values recorded by a sensor. Once the anomaly has been identified, we intend to classify the anomaly and build a topology for such behavior. This will help an analyst monitoring a smart city system to identify attacks, classify what kind of attack has taken place and act accordingly to mitigate the attack.

To better understand system behavior, we visualize the data collected by water quality monitoring sensors and present the outputs in non-linear waveform patterns. For instance, some sensors (e.g. AIT503) show sharp peaks without any fixed period or frequency. Such kinds of dynamic patterns resemble waveforms observed in prior ECG data studies (e.g. steep changes in electric potential as the heart contracts and relaxes or variations in key shapes such as amplitude of the peaks to identify any abnormality (Patterson, 1989, Wang et al., 1989)). Past ECG research also found a significant difference in the key features such as average electric potential or maximum peak amplitude in patients with abnormal heart conditions (Patterson, 1989).

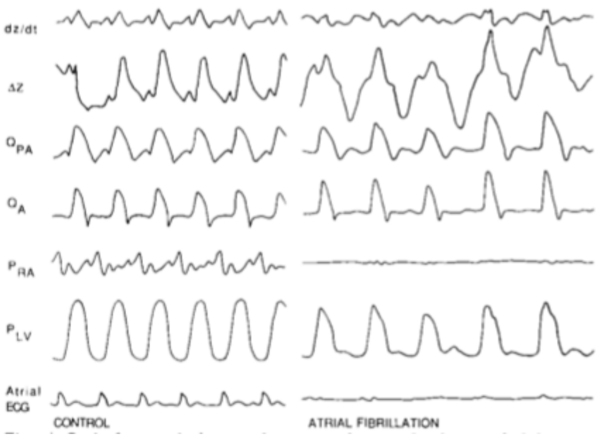

Figure 2: Left panel shows the control state in dog and right panel shows same dog after atrial fibrillation was induced. dZ/dt first derivative of the impedance change, ΔZ impedance change, Q(PA) pulmonary artery flow, Q(A) aortic flow, P(RA) right atrial pressure, P(LV) left ventricular pressure, and ECG from lead on atrium. (Patterson, 1989).

In order to establish whether the induced cyber-attacks have any impact on the sensor readings, we check for differences in the behavior of the system under attack and compare the output with the system's behavior under normal operation. Since the cyber-attack manipulates the functioning of IIoT devices and disrupts the dynamic equilibrium of the inter-connected devices, we first hypothesize that:

Hypothesis 1: During an attack the waveform generated by a sensor is different from the waveform generated by the sensor under normal conditions.

Secondly, we check whether different types of attacks (manual vs. cyber) imply different kinds of behaviors in the sensors. Although both manual and cyber-attacks disrupt the usual functioning of the system, they may, however, differ in their approach and final outcome. Therefore, our second hypothesis is:

Hypothesis 2: There is a difference in the waveforms generated by a sensor when it is under a manual attack as compared to when it is under a cyber-attack.

Solution Approach

Due to the high dimension of the data being generated every second, the data at the most granular level makes it difficult to draw useful insights and may cause us to miss out on important findings. Keeping this in mind, we analyze the data at a minute to minute level.

Attack State vs Normal State

To begin our analysis, we create a baseline of the water quality variables and take into account the measurements from the normal dataset where no attacks take place. By this, we establish a pattern for water quality behavior under normal operation of the system. In Figure 3 we analyze the behavior patterns of the four water quality analyzers (AIT501, AIT502, AIT503 & AIT504) located in part 5 of the water management system.

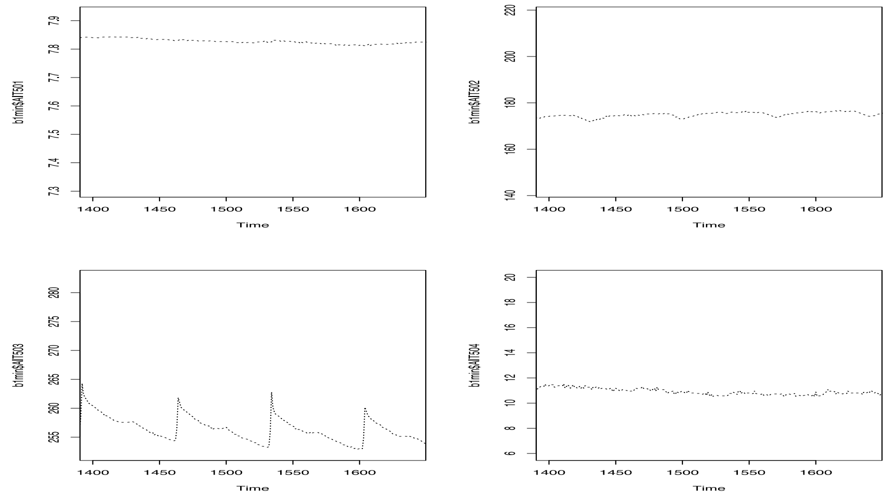

Figure 3: Water quality indicators (system under normal operation)

Once a baseline is established for all the analyzers of the system, we look at the behavior of the same four water quality analyzers under the attack. As the attack dataset also consists of intermittent intervals where no attack takes place, we first gather the time interval where each attack began and ended. By this we can accurately see and measure the behavior of the sensors that are under attack. Once the time intervals of all attacks and their corresponding targets have been established, we start looking at their behavior. Figure 4 presents an example of part 5's sensors' behaviors during an attack on the water conductivity analyzer, which measures NaCl level (AIT503). The attack begins in the 1951st minute of the experiment and ends in the 1963rd minute of the experiment:

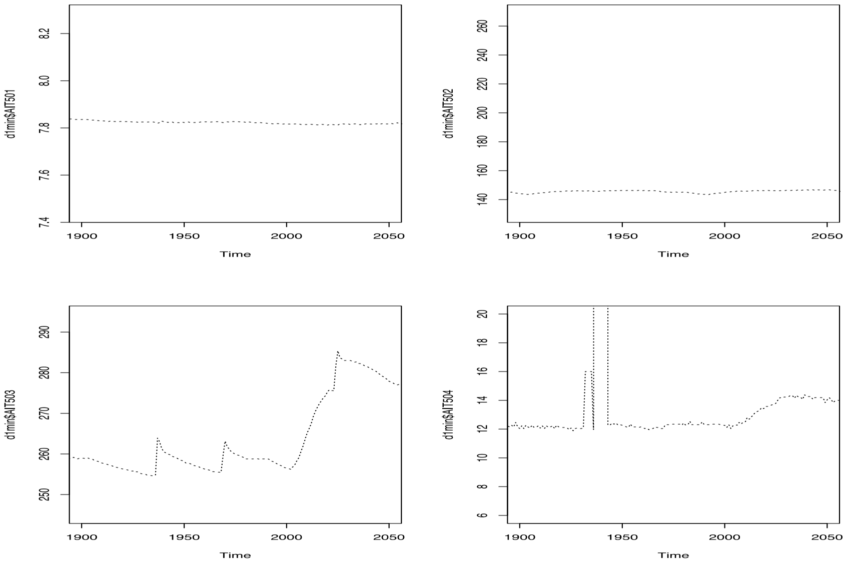

Figure 4: Water quality indicators (system under cyber-attack)

Visual inspection shows that the plots of the behavior of the analyzers clearly change when they are under attack, as compared to their normal behavior. To quantify this change in behavior and to establish that there is a statistically significant change in the sensor's behavior under attack as compared to the normal state, we conduct a sign paired t-test analysis to compare the means. The unit of analysis in this test is the sensor that is generating the digitized waveform. We compare the means of sensor readings pre and post cyber-attack incidents to test the hypothesis proposed earlier.

Physical Attack vs Cyber Attack

In the experiment two different types of attacks are carried out: physical and cyber. During a physical attack a part of the system is physically modified; for example a pump is switched off or a valve is opened. Under a cyber-attack no physical change occurs, but a part of the system may be calibrated in such a way that it only reports one value for a fixed amount of time, even though that is not the actual reading or measurement. In order to test Hypothesis 2, we analyze if waveforms generated by a sensor are different for the two different types of attacks.

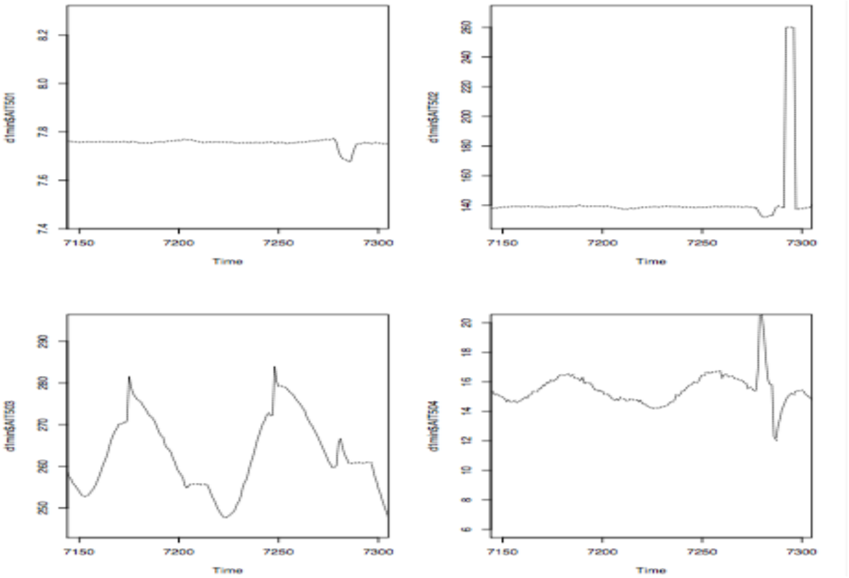

Figure 5: Water quality indicators (system under physical attack)

As presented in Figure 5, the waveforms of the sensors' readings during a physical attack look different from a cyber-attack waveform output. In order to check whether the waveforms formed during a physical attack are significantly different from the waveforms during a cyber-attack, we conduct sign paired t-tests and check if the difference of means is statistically significant.

Results

To check whether the behavior of the analyzers changes when they are under attack, we apply a sign paired t-test to check if the difference of means of the measurements collected for that analyzer with or without being attacked is statistically significant. We conclude that the difference in means is always statistically significant at α = 0.05 and our findings are as follows:

Analyzer (Sensor)	t-statistic	p-value	Mean of the differences
AIT201	108.71	< 2.2e-16	50.68
AIT202	-70.053	< 2.2e-16	-0.13
AIT401	-41.196	< 2.2e-16	-29.03
AIT402	18.429	< 2.2e-16	10.79
AIT501	56.059	< 2.2e-16	0.08
AIT503	21.383	< 2.2e-16	2.09
AIT504	-12.146	< 2.2e-16	-1.99
AIT502	44.992	< 2.2e-16	13.89

Table 3: Results of Welch t-test for all analyzers (attack vs normal)

The t-tests presented in Table 3 compare the mean of the measurement readings of an analyzer under attack to its mean of measurements collected during normal operation. This method captures the change in behavior of the sensor undergoing an attack and compares it against normal operation.

As we establish that there is a significant difference in the means of the values recorded by an analyzer during an attack as compared to normal behavior, we conclude that Hypothesis 1, stating that the waveform generated by a sensor is different from the waveform generated by the sensor under normal conditions, is supported. This finding follows closely the cardiography research where the ECG waveform of an abnormal heart condition was found to be significantly different from the ECG waveform of a regular heartbeat.

In the second hypothesis we employ the sign paired t-test presented in Table 4 to check if the mean output of a sensor under physical attack is significantly different from the mean output of a sensor under a cyber-attack. We find that at α = 0.05 there is a statistically significant difference in the means. This leads us to support Hypothesis 2, which states that there is a significant difference in behavior of sensors when they are under a physical attack as compared to a cyber-attack.

Analyzer (Sensor)	t-statistic	p-value	Mean of the differences
AIT201	564.49	< 2.2e-16	42.85
AIT202	-3.76	< 0.00044	-0.29
AIT401	2.98	0.00444	0.0019
AIT402	7.1513	< 3.48e-09	1.853
AIT501	14.893	< 2.2e-16	0.06
AIT502	3.79	0.0001869	4.439
AIT503	4.3988	< 2.061e-05	4.605
AIT504	-21.57	< 2.2e-16	-2.35

Table 4: Results of Welch t-test for all analyzers (physical attack vs cyber-attack)

Our results provide preliminary evidence of a significant difference in the features of waveforms rendered from digitized information captured by IIoT devices when they are under an attack. The psychological or externally induced abnormalities impact the waveforms of Electrocardiograms (ECGs) of a patient, while in our study the externally induced disruptions are influencing the sensor readings and the rendered waveforms. The link between cardiac abnormalities and well-defined waveforms (e.g. P,Q,R,S,T waves) in the ECGs are clearly established in the prior health care literature but to our knowledge a detailed analysis of waveforms has not been undertaken in the context of system security. These findings motivate future research for anomaly detection and real time assessment of IIoT devices for cyber threats using analytics.

Limitations and Future Work

It should be noted that there are some limitations of using a difference of means approach to establish changing behavior as the result of a cyber-attack. Our approach ignores the information in the waveform shape structure and the spiky nature of the data. The information in the peculiar shapes of the waveforms can be incorporated using advanced data mining techniques such as functional shape analysis (FSA) (Foutz, & Jank, 2010). FSA methods would also be useful in reducing noise in the sensor data by rendering the waveforms using smoothed continuous functions. In addition, a better representation of the waveforms as continuous functions would allow us to extract information related to the change in sensor readings which can assist in real time assessment of the cyber threats. We leave these propositions for our future work.

In this preliminary study of the SWaT dataset we are able to establish that there is a clear distinction in the behavior of IoT devices when they undergo an attack. Also, we observe that the two different kinds of attacks conducted in this experiment induce different behaviors from the sensors, leading us towards the next issue at hand. Going forward, we would like to make use of non-parametric methods to encode the waveforms of a sensor under attack to a linear form, which can help in identifying if an attack took place and also defining what type of attack took place. We can make use of non-parametric or functional methods to capture the shape of the waveforms and compare them in order to build a topology of waveforms undergoing different kinds of possible attacks.

Acknowledgements

Data for this research has been kindly provided by the iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design.

REFERENCES

Babaie, T., Chawla, S., Ardon, S., & Yu, Y. 2014. "A unified approach to network anomaly detection," in *Big Data (Big Data), 2014 IEEE International Conference* on (pp. 650-655). IEEE.

Bivens, A., Palagiri, C., Smith, R., Szymanski, B., & Embrechts, M. 2002. "Network-based intrusion detection using neural networks," *Intelligent Engineering Systems through Artificial Neural Networks,* 12(1), 579-584.

Cerrudo, C. 2015. "An emerging us (and world) threat: Cities wide open to cyber attacks," *Securing Smart Cities*.

DeMarzo, A. P., & Lang, R. M. 1996, September. "A new algorithm for improved detection of aortic valve opening by impedance cardiography," in *Computers in Cardiology*, 1996(pp. 373-376). IEEE.

Dominic, D. D., & Said, A. M. 2014. "Network anomaly detection approach based on frequent pattern mining technique," in *Computational Science and Technology (ICCST)*, 2014 International Conference on (pp. 1-6). IEEE.

Elfrink, W. 2012. "The smart-city solution." Retrieved from https://www.mckinsey.com/industries/public-sector/our-insights/the-smart-city-solution

Espelund, G. 2016, May 9. "How vulnerable are water utilities to traditional and cyber threats? - Environmental Science & Engineering Magazine." Retrieved from https://esemag.com/featured/how-vulnerable-are-water-utilities-to-cyber-threats/

Foutz, N. Z., & Jank, W. 2010. "Research note—prerelease demand forecasting for motion pictures using functional shape analysis of virtual stock markets," *Marketing Science,* 29(3), 568-579.

Goh, J., Adepu, S., Junejo, K. N., &amp; Mathur, A. 2016. "A dataset to support research in the design of secure water treatment systems," in International Conferenc*e on Critical Information Infrastructures Security* (pp. 88-99). Springer, Cham

Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. 2007. "Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection," *Decision Support Systems*, 43(4), 1362-1374.

Horowitz, S. L. 1975. "A syntactic algorithm for peak detection in waveforms with applications to cardiography," *Communications of the ACM*, 18(5), 281-285.

Horwitz, L. n.d. "Internet of Things (IoT) - How IoT devices lay the foundation for smart city infrastructure." Retrieved from https://www.cisco.com/c/en/us/solutions/internet-of-things/smart-city-infrastructure-guide.html

Fan, W., Miller, M., Stolfo, S., Lee, W., & Chan, P. 2004. "Using artificial anomalies to detect unknown and known network intrusions, "*Knowledge and Information Systems*, 6(5), 507-527.

Jiang, J., & Papavassiliou, S. 2004. "Detecting network attacks in the internet via statistical network traffic normality prediction," *Journal of Network and Systems Management*, 12(1), 51-72.

Jones, L. 2016, August 31. "Securing the Smart City." Retrieved from https://eandt.theiet.org/content/articles/2016/05/securing-the-smart-city/

Kim, J., Yoo, W., Sim, A., Suh, S. C., & Kim, I. 2017. "A lightweight network anomaly detection technique," in *Computing, Networking and Communications (ICNC)*, 2017 International Conference on (pp. 896-900). IEEE.

Kitchin, R., & Dodge, M. 2017. "The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention," *Journal of Urban Technology*, 1-19.

Leyden, J. 2016, March 24. "Water treatment plant hacked, chemical mix changed for tap supplies." Retrieved from https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

Maddox, T. 2016, August 1. "Smart cities: 6 essential technologies." Retrieved from https://www.techrepublic.com/article/smart-cities-6-essential-technologies/

Mills, E. 2011, November 18. "Hacker says he broke into Texas water plant, others." Retrieved from https://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/

Nakashima, E. 2011, November 18. "Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says." Retrieved from https://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html?utm_term=.e531bba76430

Oliveira, D. 2010. "Cyber-Terrorism & Critical Energy Infrastructure Vulnerability to Cyber-Attacks," *Envtl. & Energy L. & Pol'y J.*, 5, 519.

Ono, T., Miyamura, M., Yasuda, Y., Ito, T., Saito, T., Ishiguro, T., ... & Yambe, T. 2004. "Beat-to-beat evaluation of systolic time intervals during bicycle exercise using impedance cardiography," *The Tohoku journal of experimental medicine*, 203(1), 17-29.

Packer, M., Abraham, W. T., Mehra, M. R., Yancy, C. W., Lawless, C. E., Mitchell, J. E., ... & Pina, I. L. 2006. "Utility of impedance cardiography for the identification of short-term risk of clinical decompensation in stable patients with chronic heart failure," *Journal of the American College of Cardiology*, 47(11), 2245-2252.

Patcha, A., & Park, J. M. 2007. "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer networks*, 51(12), 3448-3470.

Patterson, R. P. 1989. "Fundamentals of impedance cardiography," *IEEE Engineering in Medicine and Biology magazine*, 8(1), 35-38.

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. 2016. "Special Section Introduction—Ubiquitous IT and Digital Vulnerabilities*," Information Systems Research*, 27(4), 834-847.

Rosenberg, E., & Salam, M. 2017, April 8. "Hacking Attack Woke Up Dallas With Emergency Sirens, Officials Say." Retrieved from https://www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html?_r=1&utm_source=MIT+Technology+Review&utm_campaign=056ffab32c-The_Download_2017-04-07&utm_medium=email&utm_term=0_997ed6f472-056ffab32c-154352697&mtrref=undefined

Sanger, D. E. 2016, February 29. "Utilities Cautioned About Potential for a Cyberattack After Ukraine's." Retrieved from https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html

Sanger, D. E. 2016, March 24. "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam." Retrieved from https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html

Shukla, A. 2017. "Are Smart Cities Prepared For Cyber Attacks?" Retrieved from http://businessworld.in/article/Are-Smart-Cities-Prepared-For-Cyber-Attacks-/11-07-2017-121886/

Sleptchenko, A., & Johnson, M. E. 2014. "Maintaining Secure and Reliable Distributed Control Systems," *INFORMS Journal on Computing*, 27(1), 103-117.

Speake, G. 2015, March 28. "The Proliferation Of Cyber Threats To Water And Wastewater." Retrieved from https://www.wateronline.com/doc/the-proliferation-of-cyber-threats-to-water-wastewater-0001

Thibodeaux, T. 2017. "Smart Cities Are Going to Be a Security Nightmare," Retrieved from https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare

Thottan, M., & Ji, C. 1999. "Statistical detection of enterprise network problems," *Journal of Network and Systems Management*, 7(1), 27-45.

Tian, H., & Ding, M. 2016. "Diffusion Wavelet-Based Anomaly Detection in Networks," in *Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, 2016 17th International Conference on (pp. 382-386). IEEE.

Walton, B. 2016, June 9. "Water Sector Prepares For Cyberattacks." Retrieved from http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/

Walton, B. 2017, April 6. "Water Utility Cyberattack Rings Up Hefty Data Charges - Circle of Blue." Retrieved from http://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges/

Wang, X., Sun, H. H., Adamson, D., & Van De Water, J. M. 1989. "An impedance cardiography system: a new design," *Annals of biomedical engineering*, 17(5), 535-556.

Wang, W., Guan, X., & Zhang, X. 2004, August. "A novel intrusion detection method based on principle component analysis in computer security," in *International Symposium on Neural Networks* (pp. 657-662). Springer, Berlin, Heidelberg.

Wu, J., Ota, K., Dong, M., & Li, C. 2016. "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, 4, 416-424.