Texas A&M University at Qatar

ECEN 403 - Electrical Design Lab 1

Semester: Fall 2019

Project Proposal

Anomaly detection in BACnet protocol systems

Team Members: Sofian Ghazali

Muhammed Zahid Kamil

Rahul Balamurugan

Project Mentors: Dr. Hussein Alnuweiri

Mr. Salah Hessien

Submission Date: 09/09/2019

"An Aggie does not lie, cheat, or steal, or tolerate those who do."

Table of Contents

Abstract

Building Automation Networks/Systems (BAN/BAS) are networks that control and monitor utilities and equipment in smart buildings. The BACnet protocol is one of many communication protocols for smart networks and is widely used as a BAS communication standard. As the number of utilities and buildings connected by such Wide Area Networks increases, the need for robust cyber-physical security measures also increases. Although much research has been done on the subject, constant developments in BAS technology implies similar need for advancement in security as well.

In this project, we propose to generate large amounts of data by emulating a real BAN on Raspberry Pi stacks, so as to develop an anomaly detection method using semi-supervised machine learning. The anomalies could be synthetic attacks or malfunctions in BAN services. This shall build upon concepts developed by other researchers in the field, specifically the THE (Time-driven, Human-driven, and Event-driven) classification of network traffic, and machine learning techniques by various researchers. The end product should be an anomaly detector that is resilient, adaptive, responsive to zero-day attacks, and have a small false-alarm rate. The focus is on reducing labeling work and improving accuracy by merging supervised and unsupervised techniques to create a unique program. The network anomaly detector shall be well tested by subjecting the BACnet stack to synthetic attacks.

Introduction

Building Automation Systems (BAS) are computer-based control systems installed in large buildings to achieve autonomous control of the entire facility. BAS was made for convenience and later required remote access instead of installing software on specific Personal Computers (PCs). Communication between the building utilities/devices are achieved via Wide Area Networks (WAN) which also provide remote access for facility managers to monitor their equipment (air conditioning, ventilation, lighting etc.). An example of such a network would be the Building Automation Control network or BACnet [1], one of the leading Internet Protocol (IP)-based network technologies in the field and the focus of this research. However, exposure of the devices and servers to the WAN make them vulnerable to cyber-attacks due to their IP addresses being relatively easy to discern [2]. Hackers could use the BAS as a point of access to obtain sensitive data related to the company and its customers. For example, the attack in the Target stores in 2013 where criminals achieved access to millions of credit and debit card accounts by stealing login credentials of Target's ventilation and air conditioning systems [3].

Search engine tools such as Shodan and Censys [4] for searching internet connected devices can become platforms for hackers to access BAS systems from the public internet. Cobb [5] was able to generate a scale of 21,000 potential targets of BAS systems by the end of August 2018 using these search engines. With so many potential BAS system targets for hackers to choose from, such as clinics, hospitals, universities and even a few banks, sensitive information of many individuals could be obtained. Hackers could also hold companies for ransom by damaging their reputations, causing financial loss and/or security issues, or disrupting normal facility operations [6]. This underlines the need for robust cyber-physical security for BAS systems.

Current solutions and research have been focused on using anomaly detection and Intrusion Detection Systems (IDS) to improve system resilience and device-level security management. Some existing anomaly detection methods are the timing-based detector for cyber-physical systems (CPS) by Zimmer et. al [7], and the finite states-based detector for Modbus networks by Goldberg et. al [8]. The major challenge faced by researchers in anomaly detection is to minimize the number of false alarms and improve their efficiency. In this regard, Zheng and Reddy, researchers at TAMU College Station, formulated a THE-driven anomaly detector for BACnet that uses frequency analysis [9]. The system classifies network traffic into THE: *Time-driven, Human-driven, and Event-driven* categories, which makes for a comprehensive network traffic model, enabling different mechanisms to detect for anomalies in each category.

Although Zheng et. al's detector model is novel and effective, current rate of increase in data size of BACnet networks [10] warrant a need for an automated and unsupervised system. This project will plan to follow up on this research by using machine learning techniques instead of Fourier frequency analysis to capture normal data patterns and detect anomalous traffic. Previous research in the usage of machine learning to detect network anomalies is rather extensive such as the work of Tonejc et. al [11] in characterizing BACnet network traffic data by means of unsupervised machine learning techniques. Thus, the aim of this project is to use the classification system proposed by Zheng et. al and the methods discussed by Tonejc et. al to create our anomaly detection system. This would fall under the category of semi-supervised [12] machine learning techniques, eliminating both the higher error probabilities of unsupervised methods [13] and the need for an enormous amount of data and time resources that characterize supervised learning methods [14].

This paper presents an overview of Building Automation Systems, the BACnet protocol, machine learning methods in network anomaly detection, our methodology, the details of the proposed project, and the expected outcomes in the next section. Further sections contain the budget for the project and project timeline.

Proposed Design

Objectives

Our goal is to implement THE-driven semi-supervised Machine Learning (ML) techniques to allow for automated anomaly detection in BACnet traffic and ensure that this procedure alerts the user of an imminent attack on the hardware system. We aim to gather large amounts of data, sufficient for ML algorithms carry out large scale inspection of anomalous data patterns.

The specific list of objectives that we intend to meet are:

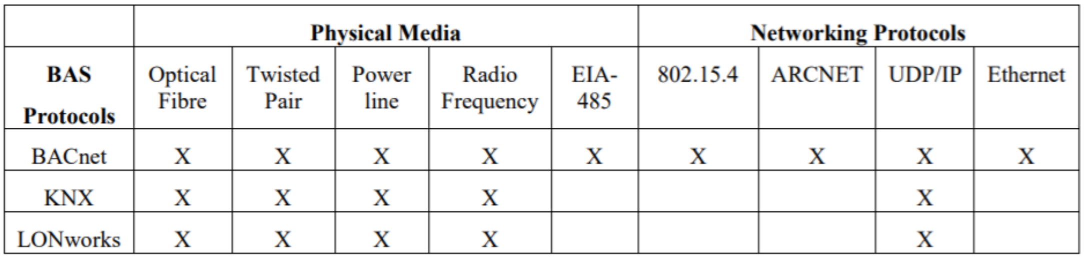
1. To examine and understand traffic behavior in BAS systems
2. To assess the feasibility of ML algorithm when exposed real-time traffic networks.
3. To identify methods of classifying and inspecting data packets via different types of ML models.
4. To investigate the different types of cyber-attacks and measure the accuracy rate of our algorithm

To address these objectives, we aim to conduct three phases of research spanning an entire year. This includes, 1.) Gathering large sources of data necessary for training phase of the algorithm; 2.) Conduct extensive testing on synthetic network traffic to evaluate our model; 3.) Optimize the system to meet a certain threshold accuracy to be deemed fit for use in real-time BAS traffic systems.

BACnet Protocol Overview

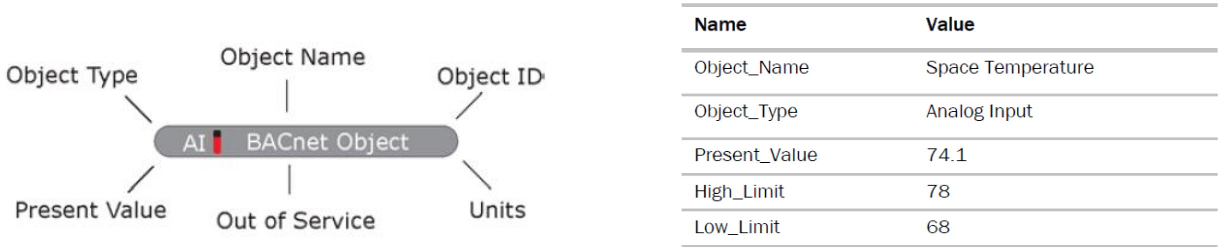
Building Automation Systems (BAS) were not designed by considering security as a priority and its devices were expected to last more than a decade (up to 15-20 years) that over time would make BAS more vulnerable and require updates [15]. BACnet is a data communication object-oriented protocol that enables interoperability between different building systems and devices in BAS. BACnet is a versatile protocol working over multiple physical media and networking protocols compared to the other protocols such as KNX and LONworks [16].

Table 1: Comparison of BAS protocols [16]



	Physical Media					**Networking Protocols**			
BAS Protocols	Optical Fibre	Twisted Pair	Power line	Radio Frequency	EIA-485	802.15.4	ARCNET	UDP/IP	Ethernet
BACnet	X	X	X	X	X	X	X	X	X
KNX	X	X	X	X				X	
LONworks	X	X	X	X				X	

BACnet can be further classified as BACnet objects, BACnet Services and BACnet properties. BACnet objects comprise of a collection of properties. For example, common BACnet properties are the object’s name, type, value, upper and lower limits [17]. Examples of object types include *Analog/Binary input, analog/binary output, device etc*. BACnet services are used to exchange information between BACnet objects that can be further classified into the following categories: object access, device management, alarm and event, file transfer and virtual terminal.



Name	Value
Object_Name	Space Temperature
Object_Type	Analog Input
Present_Value	74.1
High_Limit	78
Low_Limit	68

Figure 1: BACnet objects and its properties [17]

The main interoperability aspect of BACnet are the ReadProperty and WriteProperty. The WriteProperty enables the client device to write(change) a property of an object in the server device. If there is a need to for multiple clients to write to the same property then there is a command priority mechanism. This priority setting has levels from 1 to 16 where 1 is the most important and 16 is the least important. This mechanism is useful in detecting any cyber criminals as they may try to increase the level of priority for the unauthorized access of the BACnet device. BACnet also provides a Change of Value (COV) aspect to mitigate traffic so that only if the value of the object property changes more than its trigger amount then the server issues a COV notification.

BACnet/IP protocol is a high-speed network for high level communications over local IPs and Wide Area Networks (WAN). The BACnet/IP network is a virtual network that uses BACnet broadcast messages which are the Who-is and I-am services to obtain the unique device addresses.

BACnet uses a collapsed 4-layer network architecture (see Figure 3) and also has its own Network Security definition which allows standard BACnet messages to become secure.[18] This BAS protocol has a much wider security implementation compared to KNX and LONworks with the addition of the BACnet Security Services (BSS) [16]. The BSS provides encryption such as Advanced Encryption Standard (AES), Key Hashed Message Authentication Codes and Secure hash Algorithm 256bit.

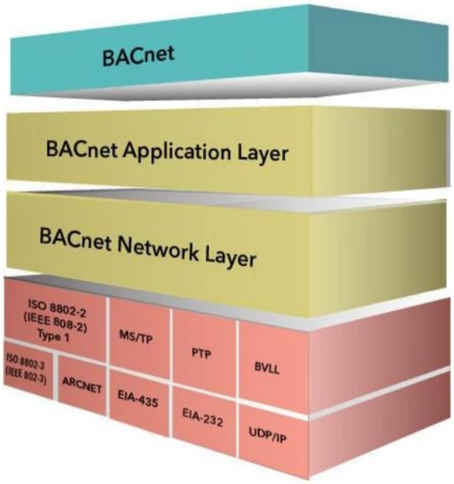


Figure 2: BACnet network architecture [20]

Limitations

1. BSS is an optional feature of the BACnet protocol and has not become a commercially available product [16]
2. BACnet Web Services, BACnet/WS that can implement security protocols such as TLS (Transport Layer Security) and HTTP (Hypertext Transfer Protocol) is not available for all BACnet devices [18].
3. Real-time datasets cannot be obtained conveniently so this project will resort to obtaining data from online databases and mimicking different scenarios by generating different data packets.

Threat Models

The most common network attacks that exists for a BACnet device are as follows:

DDoS attacks: Distributed Denial of Service attacks are the most common type of attacks on an inter-connected system such as BACnet. DoS can result from smurf attacks, router advertisement flooding etc. [9] A DDoS attack is a malicious attempt to disrupt normal traffic and flood a network with so much traffic that it slows down the connectivity of legitimate users to the network. A prominent case of a DDoS attack was in eastern Finland where the central heating and water systems were shut down for 60,000 residents [19]. This represents a need to introduce tighter security measures in BAS systems.

Man in the Middle: This type of attack involves an attacker secretly relaying and intercepting communication between two parties directly communicating with each other.

Data tampering: This is the act of deliberately modifying the data through unauthorized channels. The intent is purely malicious and is one of the biggest threats to any organization. This attack is frequently present in BAS systems and is a prime example of a human-driven traffic interception.

Data ex-filtration: This attack involves copying and transferring of data from a computer or a server. It can be performed by an individual with physical access to a computer or building system. It is a difficult domain to detect since most of this attack mimics normal traffic.

Methodology

Our methodology is comprised into the following 4 sections:

Collecting training data

To collect our training dataset, we rely on two sources: Packet Analyzer software such as Wireshark and a pre-collected dataset from existing projects. We received a pre-collected dataset from TAMU where a similar research has been carried out. This is a huge amount of data that is unlabeled which will be useful for Machine Learning. The second source relies on Wireshark application that will be able to show the BACnet data packets generated from the Python-run Raspberry Pi 3 controllers. The datasets will be labelled and preprocessed into a CSV file format to be fed into the Machine Learning algorithm.

BACnet Traffic Classification

We propose to use the THE-driven traffic classification system developed by Zheng et. al [9] as it is comprehensive and easy to interface with labels for machine learning later on. THE stands for Time, Human and Event -driven traffic. Network traffic on BACnet systems either fall in one of the categories mentioned above or in a combination of two or all of them. We plan to identify the percentage of each request type in each category and label them accordingly. Below is the explanation of the three categories:

Time-Driven: This traffic is generated by scheduled services, and as such is not supposed to be affected by real-time network events. Classifying this data type separately allows us to examine if there is a delay in the network packets and extract timestamps (the time at which BAC device delivers the data). Delays generally occurs due to some data tampering from the BACnet devices.

Human-Driven: This type of network traffic is generated by humans and is often non-periodic. It can happen at any stage and it only constitutes 5% of the total BACnet traffic [20]. Human-driven network traffic typically involves change of value on objects; in other words, a malicious user tries to alter the data in physical devices such as temperature or light intensity. A particular service request called WP (Write Property) allows data to be changed and this must be immediately identified so as to prevent malfunction of devices.

Event-driven: This category consists of network traffic generated due to change-of-state events, such as alarms, device feedback upon change in value (ON/OFF/set) and system status alerts.

Detecting Anomalous Behavior

The concept of network anomaly detection using machine learning techniques has been well researched over the past decade. Some of the works we reviewed are the usage of unsupervised techniques by Tonejc et. al (clustering, random forests, one-class support vector machines, and support vector classifiers) [11], Lane et. al’s similarity measuring method [21], and general methods from Bhattacharyya and Kalita’s book [12] on the topic. Although the specific workings are different, anomaly detection using machine learning is based on the program detecting the degree of variation from expected data patterns and evaluating them [12]. Moreover, the focus is on building up a sufficient library of BACnet traffic data for the program to learn and analyze.

Given the large amount of network traffic data and the vast amount of IP packets that are produced every minute from the BACnet systems, we aim to classify these datasets using the Semi-supervised learning.

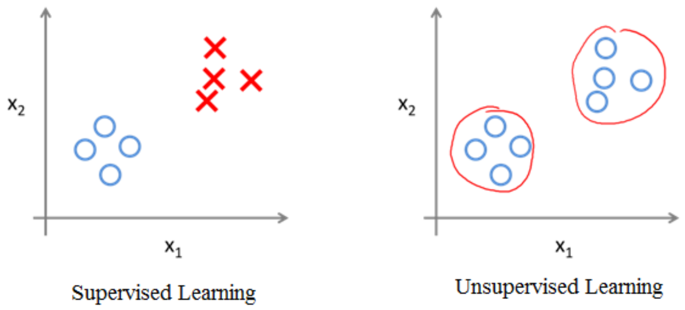


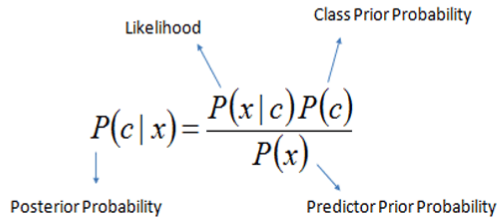
Figure 3: Visual representation of Supervised and Unsupervised Learning [16]

Semi-Supervised learning is the hybridization of Supervised and Unsupervised learning techniques. Supervised learning makes use of labeled training dataset and trains to map the input to the output using specialized computing techniques. In contrast, Unsupervised learning involves modeling an unlabeled dataset to try find a hidden structure or pattern to understand about the dataset. Supervised learning method benefits from the fact that the algorithm implementing this method already knows what type of output to expect and often results in lower error rate. However, when exposed to real-time (unseen data) that doesn't belong to any of the classes from the training dataset, the output may be a wrong class label. In the case of Unsupervised, the algorithm classifies or clusters data by discovering features on its own. When dealing with BACnet traffic data, we have an issue of handling many data packets and manually labeling a huge dataset is going to be cumbersome and costly. In this case, carrying out only supervised learning won't suffice on its own. Alternatively, we cannot feed data packet datasets into ML algorithms without pre-processing. However, pre-processing a random cluster of data for unsupervised learning without any forethought would render futile unless we know what each segment of a data packet represents. To find a trade-off between these two approaches, Semi-supervised learning comes in handy. This approach uses a small amount of labeled data with a large amount of unlabeled data. The main aim behind this approach is for the algorithm to infer the correct labels for an unlabeled dataset. Unsupervised learning is needed to cluster similar data according to their unique features. Supervised learning is needed to use the labeled data to infer the labels of the rest of the dataset.

The types of Machine Learning techniques we will use are the following:

Naive Bayes Classifier

This is a classification technique heavily inspired from the Bayes Theorem. This technique relies on the assumption of independence of events (events in this case is the dataset features). Even though features of a specific data might be related to another, Naive Bayes considers them separate. It is a useful technique for very large datasets, and since BACnet network traffic dataset is large, this technique would prove useful.



$$P(c \mid x) = \frac{P(x \mid c)P(c)}{P(x)}$$

$$P(c \mid \mathrm{X}) = P(x_1 \mid c) \times P(x_2 \mid c) \times \cdots \times P(x_n \mid c) \times P(c)$$

Figure 4: Bayes Theorem Formula [22]

From the equation,

P(c|x) = Probability of target variable (c) given a feature (x)

P(c) = Probability of a target

P(x|c) = Probability of a feature (x) given a target ©

P(x) = Probability of a feature

Support Vector Machine (SVM)

This is again a classification technique and here we plot the datasets as points in a n-dimensional space where n represents the number of features. The value of each feature is represented as a particular coordinate. The clustering effect allows for points to form discrete clusters that are close to each other and will likely share the same label. After representation on an n-dimensional space, a line is plotted in such a way that it splits the data into two differently classified groups of data, according to their respective features. Although there are many hyperplanes (n-dimensional) that can be drawn, the best choice will be the hyperplane that leaves the maximum margin or distance from both classes.

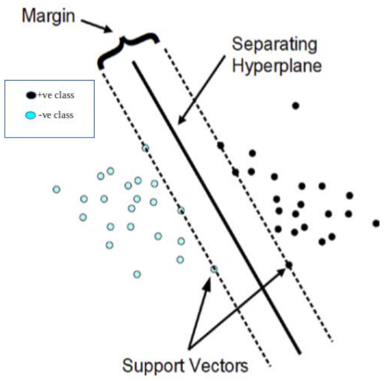
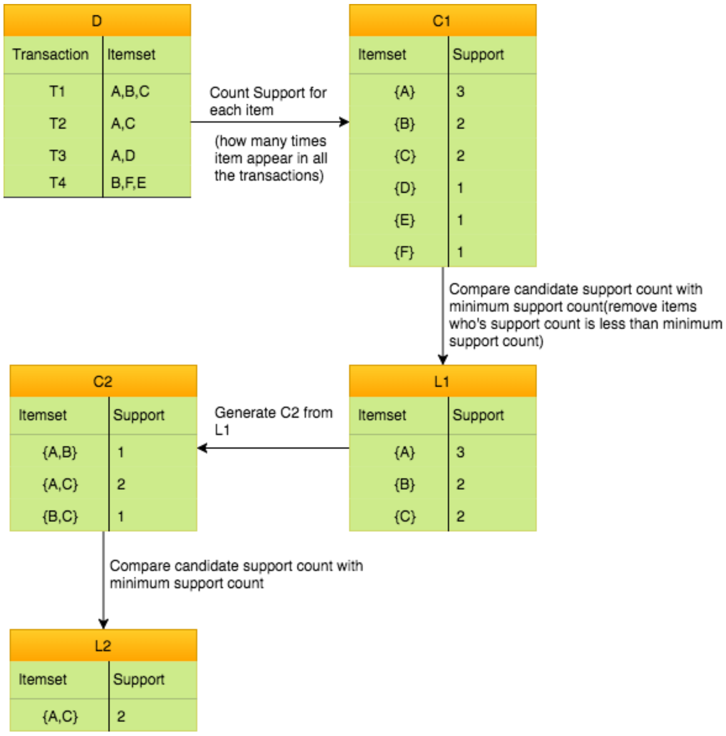


Figure 5: Visual representation of Support Vector Machine [23]

Apriori Algorithm

This is a prevalent unsupervised algorithm that generates association relationships between features on a given dataset. For example, if feature A occurs, then feature B occurs based on a probability. The algorithm will first find out pattern between sets of data and compute a ratio. In the case of BACnet traffic dataset, if the service request “WP” (write property) occurs a number of times with a particular IP address of a device, then BMS managers can predict that the device is under risk of data tampering.



D

Transaction	Itemset
T1	A,B,C
T2	A,C
T3	A,D
T4	B,F,E

Count Support for each item

(how many times item appear in all the transactions)

C1

Itemset	Support
{A}	3
{B}	2
{C}	2
{D}	1
{E}	1
{F}	1

Compare candidate support count with minimum support count(remove items who's support count is less than minimum support count)

L1

Itemset	Support
{A}	3
{B}	2
{C}	2

Generate C2 from L1

C2

Itemset	Support
{A,B}	1
{A,C}	2
{B,C}	1

Compare candidate support count with minimum support count

L2

Itemset	Support
{A,C}	2

Figure 6: Apriori Algorithm concept [24]

Testing

The BACnet system designed for data generation will be subjected to synthetic attacks to test the resilience and response of the anomaly detector. The attacks will encompass the main threats to BACnet systems, such as DDoS attacks, Data tampering, and Data-exfiltration.

Design Details

The project will mimic 4 towers sending BACnet messages to the other towers using BACnet/IP protocol. The towers are Virtual Local Area Networks (VLANs) that will be connected to each other using an interVLAN router (CISCO Catalyst 3750). Each tower will have 8 floors (8 raspberry pi’s as 1 stack) with each raspberry pi as a BACnet device having a unique ID.

BACnet/IP protocol will require ethernet cables for each stack and python will be used to generate the random data packet to the random BACnet device. Wireshark will be used to record and check for the BACnet data packets that will be later used for labelling once Machine Learning is being implemented.

BACnet protocol will also follow the standards of The American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE). For example, [25] informs when should the server send a COV notification in order to reduce the burden on the server.

The different scenarios and vulnerabilities such as Energy-demand shock, building driven to extreme temperatures, HVAC (Heating Ventilation and Air Conditioning) failure will be mimicked for detection implementations. However, fine-tuning an IDS (Intrusion Detection System) is a manual process therefore, machine learning algorithms can be applied for data packet classification and profiling [26].

Machine Learning will use datasets from online databases to identify and label the data packets that will be preprocessed to parse network packets into a CSV file. Another source of data will be artificially generated data packets.

Anticipated Results and Learning Outcomes

The results at the end of the project should include a significant library of BACnet traffic data generated and labeled according to the THE-driven model; a novel anomaly detection method using semi-supervised machine learning techniques; and the successful testing of the anomaly detector against multiple synthetic attacks targeting the simulated BACnet stack.

Over the course of the project, the technical skills we gain would be: usage of machine learning techniques, building and maintaining a BACnet network, troubleshooting network issues, and general project management skills. Additionally, we would learn to research and review solutions to our problems, ask critical questions and work effectively as a team.

Estimated Budget and Justification

The only components that need to be purchased are the hardware parts, the details of which are provided in the table below. They are necessary to be purchased at the earliest since it is expected to take up to six months of runtime to accumulate enough network data to teach the anomaly detector.

Table 1: Budget Outline for the project

Component	**Quantity**	**Approximate Price**
Raspberry Pi 3	32	$35x8 = $280
8-layer Dog Bone stackable case	4	$33.51x4 = $134.04
Cisco Catalyst 3750 48 port	1	$87.46
		Total ≈ $500

Project Timeline

	September				October					November				December	
Project Proposal and Team Working Agreement	🟦	🟦													
Project Proposal Presentation Preparation		🟩	🟩												
Project Website Preparation			🟪	🟪											
Raspberry pi stack implementation				🟥	🟥	🟥	🟥	🟥							
BACnet implementation of 4 VLANs							🟦	🟦	🟦	🟦	🟦				
Testing											🟧	🟧	🟧	🟧	🟧
Education on Machine Learning					🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Progress Presentation Preparation												▨	▨		
Final Presentation and Report												🟦	🟦	🟦	🟦

Conclusion

BACnet networks are security-critical, as they control private and essential services. These are under threat due to exposure on the WAN i.e. internet. This project will provide a part of the solution against cyber-physical threats by detecting the existence of anomalies on BACnet networks. To build the detection program, we will use the THE-driven classification model and semi-supervised machine learning techniques. The program will be trained on real-time data generated by running a BACnet stack emulation as well as available resources online. This concept model will be tested after the training phase by generating synthetic attacks. This project has the potential to be developed further by focusing on reacting retroactively to the pre-existing and unknown anomalies of the network traffic.

Overall, it is possible to visualize that by the end of this project, a strong grasp of BAS with the implementation of ML techniques can result in automatically detecting new BAS attacks to compete against the ‘evolving’ cyber criminals.

References

[1] Real Time Automation (2014).”BACnet”. [online] Available at: https://www.rtautomation.com/wp-content/uploads/2014/07/BACnet_R31.pdf. [Accessed 8 Sep 2019].

[2] S. Keoh. “Cyber-physical Systems are at Risk,” Next-Gen Infosec, Jun 15, 2018. [online] Available at: https://www.infosecurity-magazine.com/next-gen-infosec/cyberphysical-systems-risk-1/ [Accessed 7 Sep 2019].

[3] Hayden, E. (2019). *An introduction to building management system vulnerabilities*. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/tip/An-introduction-to-building-management-system-vulnerabilities [Accessed 7 Sep. 2019].

[4] Censys search data. [online] Available at: https://censys.io/ipv4/metadata?q=bacnet& [Accessed 8 Sep 2019].

[5] S. Cobb (2019). *Siegeware: When criminals take over your smart building | WeLiveSecurity*. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2019/02/20/siegeware-when-criminals-take-over-your-smart-building/ [Accessed 7 Sep. 2019].

[6] Sentryo. (2019). *BMS and cybersecurity: smart systems faced with the challenges of industrial cybersecurity*. [online] Available at: https://www.sentryo.net/bms-smart-systems-challenges-industrial-cybersecurity/ [Accessed 7 Sep. 2019].

[7] C. Zimmer et. al, “Time-based intrusion detection in cyber-physical systems,” in *ICCPS’10 Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, Stockholm, Sweden, April 13-15, 2010*, ACM, New York, USA, 2010, pp. 109-118.

[8] N. Goldberg et. al, “Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems,” *International Journal of Critical Infrastructure Protection*, vol. 6, issue 2, June 2013, pp. 63-75. [online]. Available at: https://www.sciencedirect.com/science/article/pii/S1874548213000243. [Accessed 8 Sep 2019].

[9] Z. Zheng and A. Reddy, “Safeguarding Building Automation Networks: THE-Driven Anomaly Detector Based on Traffic Analysis,” 2017. [Online]. Available: http://cesg.tamu.edu/wp-content/uploads/2018/01/ICCCN-Zhiyuan-Zheng-Paper-2017-July-1.pdf. [Accessed: 08- Sep- 2019].

[10] S. Lyons, “Current Status of Cyber Security in the BAS Industry,” *Cimetrics February 2019 Newsletter*, Mar 1, 2019. [online]. Available at: https://www.cimetrics.com. [Accessed 8 Sep 2019].

[11] J. Tonejc et al, “Machine Learning Methods for Anomaly Detection in BACnet Networks,” *Journal of Universal Computer Science*, vol. 22, no. 9 (2016), 1203-1224. [online] Available at: https://pdfs.semanticscholar.org/d823/6a08011ad5f33e5d5c8f20d87c85a08bf784.pdf [Accessed 8 Sep 2019]

[12] D. Bhattacharyya and J. Kalita, “Introduction,” Network Anomaly Detection: A Machine Learning Perspective, New York: CRC Press, 2014, pp. 1-13.

[13] P. Liang and D. Klein, “Analyzing the Errors of Unsupervised Learning,” CS Division, EECS Department, Univ. of Cali., Berkeley, CA 94720, USA, June 2008. [online] Available at: https://pdfs.semanticscholar.org/038a/fe82cc61215e9087e572d8aab9663c1bdb0f.pdf. [Accessed 8 Sep 2019]

[14] S. Kotsiantis, “Supervised Machine Learning: A Review of Classification Techniques,” *Informatica* 31, 2007, pp. 249-268. [Online]. Available at: http://www.informatica.si/index.php/informatica/article/viewFile/148/140.[Accessed 8 Sep 2019]

[15] Chipkin Automation Systems. (2019). *How is BACnet Vulnerable?*. [online] Available at: https://store.chipkin.com/articles/how-is-bacnet-vulnerable [Accessed 7 Sep. 2019].

[16] M. Peacock and M. Johnstone, “An analysis of security issues in building automation systems,” pp. 100–104, 2014.

[17] Dms.hvacpartners.com. (2019). *Bacnet Basics User's Guide*. [online] Available at: https://dms.hvacpartners.com/docs/1000/Public/04/11-808-417-01.pdf [Accessed 3 Sep. 2019].

[18] Ccontrols.com. (2019). *Addressing IP Security Concerns when Deploying a BACnet System*. [online] Available at: https://www.ccontrols.com/enews/2018/0418story3.htm [Accessed 9 Sep. 2019].

[19] L. Mathews, “Hackers Use DDoS Attack To Cut Heat To Apartments,” *Forbes*, 08-Nov-2016. [Online]. Available: https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#25174d161a09 . [Accessed: 08-Sep-2019].

[20] Cimetrics. (2019). *uBACstac - BACnet Protocol stack for small devices*. [online] Available at: https://www.cimetrics.com/products/products-bacnet-ubacstac [Accessed 8 Sep. 2019].

[21] T. Lane and C. Brodley, “An Application of Machine Learning to Anomaly Detection.” School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907-1287. 14 Feb, 1997.

[22] V. Jha, "Naive Bayes - machine learning algorithm for classification problems", *TechLeer*, 2019. [Online]. Available: https://www.techleer.com/articles/200-naive-bayes-machine-learning-algorithm-for-classification-problems/ . [Accessed: 08-Sep- 2019].

[23] K. Kumar Mahto, "Demystifying Maths of SVM — Part 1", *Medium*, 2019. [Online]. Available: https://towardsdatascience.com/demystifying-maths-of-svm-13ccfe00091e . [Accessed: 08- Sep- 2019].

[24] "Apriori Algorithm - Last Night Study", *lastnightstudy*, 2019. [Online]. Available: http://www.lastnightstudy.com/Show?id=68/Apriori-Algorithm. [Accessed: 08- Sep- 2019].

[25] Ashrae.org. (2019). *Interpretations for Standard 135-2016*. [online] Available at: https://www.ashrae.org/technical-resources/standards-and-guidelines/standards-interpretations/interpretations-for-standard-135-2016#targetText=Interpretation%20135%2D2016%2D7%20%E2%80%93,regarding%20DeviceCommunicationControl%20for%20BACnet%20Router .) [Accessed 8 Sep. 2019].

[26] "Hands-on Machine Learning on Google Cloud Platform", *Subscription.packtpub.com*, 2019. [Online]. Available: https://subscription.packtpub.com/book/big_data_and_business_intelligence/9781788393485/6/ch06lvl1sec39/supervised-and-unsupervised-machine-learning . [Accessed: 08- Sep- 2019].