Texas A&M University at Qatar

ECEN 403 - Electrical Design Lab 1

Semester: Fall 2019

Benchmarking Analysis Report

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: 11/11/2019

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

TABLE OF CONTENTS

Introduction

Our goal in this project is to make a robust automated intrusion detection algorithm for BACnet Systems capable of alerting users of a potential data breach. We are aiming to use diverse range of Machine Learning techniques to capture normal data patterns from BACnet traffic and classify the traffic for detection of anomalous data packets. We plan to discuss the existing solutions pertaining to our project and highlight some criterias that can used to evaluate the performance of our project with that of existing solutions. Many advancements have already been made in the field of anomaly detection and we aim to explore how well other solutions perform and how we can benefit from it.

Our Proposed Engineering Design Solution

BACnet is a data communication object-oriented protocol that enables interoperability between different building systems and devices in BAS. In our design we aim to use raspberry pi towers to mimic buildings where each raspberry pi is a unique BACnet device providing information that will be useful for building managers.

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 as shown in Figure 1 below.

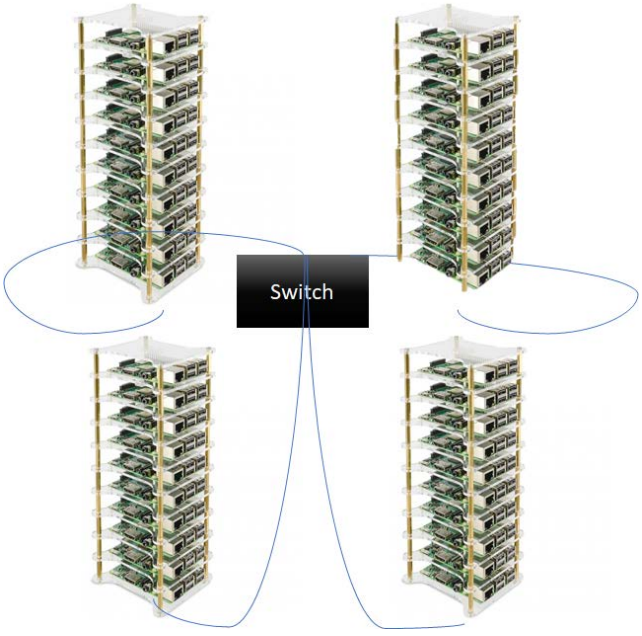

Figure 1: Proposed Design Solution

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, [5] 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 and therefore, machine learning algorithms can be applied for data packet classification and profiling [6].

Machine Learning will use datasets from acquired 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.

The final anomaly detection program should be capable of analyzing network data packets and optimizing itself where it is implemented. The program should then be able to identify any anomalies in the analyzed data with as low of a false positive rate as is possible. This end product is limited by our low level of expertise in software development and the use of generic machine learning tools. Also, the false positive rate is unavoidable to a certain extent as the network data is inherently random. However, it has to be mentioned that the use of machine learning has been aimed at minimizing the known errors and figure out as many other sources of error as we can through trial and error over a very high number of iterations. If possible, we are also looking at adding a self-updating feature to the program, the difficulty of which makes it something that will only be possible if we are well ahead of schedule. Compared to other products on the market though, our program should be more flexible and adaptive upon implementation.

Existing Solutions

The issue of security in building networks is becoming far more widely discussed than it was a few years ago due to the rise in the number of automated and connected buildings. Being one of the most widely used BAN protocols, BACnet has been at the forefront of this discussion. Though BACnet has basic encryption as an option (BACnet/SC, aka secure connect), it is not widely used due to interoperability issues and as such is not the focus of our project (which is BACnet/IP). The majority of BAN communication otherwise is in cleartext. The following are some of the solutions to the issue of lacking security in BACnet and/or other Building Automation Networks that we could find online:

- Password protection
- AC2000 BACnet Interface

- THE-driven anomaly detector by Zheng et al.
- Timing based detector for cyber-physical systems by Zimmer et al.
- Finite-state based detector for ModBus detectors by Goldberg et al.
- Unsupervised machine learning techniques, tested by Tonejc et al.

Password Protection

The main method used in securing building networks is password protection, with either a full access or multi-level access with different permission levels. The issue with this method, according to engineers in the field, is that the control of the passwords is not strict during the setting up and maintenance of the system. Also, due to mismanagement, the passwords may easily get leaked. As most, if not all, BAN devices are made to be easily discoverable and accessible, the method of password protection is not all that strong against a targeted attack.
The systems engineers responsible for setting up building automation networks are often contracted to monitor the network for any anomalous status alerts, alarms or malfunctions. This is a task that is becoming extremely tedious as the size and scale of BANs are going up fast.

AC2000 interface

This interface from Tyco Security Products enables alarms to be sent in BACnet protocol to third party systems including building management systems, HVAC, fire and any other systems that support BACnet communication. The interface is bi-directional, allowing for both the sending of AC2000 alarms and the receipt of third-party Change of Value (COV) BACnet messages, which can then be displayed on the AC2000 Security Hub alarm and event management application. As a security tool, this interface is quite versatile and is able to detect many common threats to BANs. However, from the parameters of data it monitors, it can be seen that the tool would be unable to do much in the face of a Denial of Service attack or a Man-in-the-Middle attack. The former depends exactly on the bandwidth being occupied by COV messages or alarms to break into BACnet systems, while the latter would in all probability go unidentified.

THE-Driven Anomaly Detector

Zheng et al.[2] designed and developed this detector in 2017 based on a novel network traffic classification model they called the ‘THE-driven classification method’. In this technique, all communication traffic are classified into: 1. Time-driven, 2. Human-driven, and 3. Event-driven categories. Time-driven traffic is normally generated by scheduled control programs that trigger service requests according to different timers. Such traffic presents time regularity and is not affected by real-time events of the network. Human-driven traffic includes requests that are directly generated by humans or through control programs. Event-driven traffic includes service requests that are not generated by timers or humans, but as responses to certain programmed events. The classified network traffic, in this method, is then parsed for suspicious data packets and all such anomalies are flagged. The testing information for this as reported by Zheng et al. put its accuracy above 96% across all the tested attacks. It also purportedly has a near 100%

anomaly capture rate with the exception of DoS attacks, which can be identified via other network volume-based detection techniques.

Timing-based detector

This detector works on the principle of utilizing information from static timing analysis to identify unauthorized instructions in real-time cyber-physical environments. In the case of building automation systems, the timing bounds in code segments are said to be easily available, thereby facilitating this particular method. The paper by Zimmer et al. [4] describes this mechanism which works by checking those bounds and implements the detection techniques either by itself in a self-checking manner, or through the operating system scheduler.

Finite-states based Detector

Goldenberg et al.[3] modeled a detector meant for the Modbus network protocol (and can be used in BACnet as well) based on identifying the unique deterministic finite automation “state” (DFA) of each individual channel between a HMI-PLC (Human-Machine Interface & Programmable Logic Controller) pair. The DFA is a finite-state machine that can accept or reject a given string of symbols and jumps from one state to another. It takes around 100 captured messages to identify the DFA for a given channel. This method purportedly is highly sensitive while having very low false positives. The paper mentions that Goldenberg et al. found zero false alarms over 111 hours of continuous operation.

Unsupervised Machine Learning Detector

Unsupervised ML techniques such as k-means, clustering and random forests were used by Tonejc et al. [1] to detect anomalies in building automation networks. The model was trained from two different datasets. One of which is from two days worth of network traffic from a BAS lab setup that contains about 20 different BACnet devices. The other was a dataset from artificially generated network traffic by obtaining network traffic from a different day and adding variations in the synthetically generated anomalous traffic. Clustering methods such as k-means are used to detect known attacks from the training data. Random Forests and Support Vector Machines (SVM) were used to detect new attacks.

Benchmarking Criteria

The products discussed above have their individual strong points as well as some shortcomings. In this section we introduce the list of criteria we used to contrast and compare those security solutions with themselves and with our own program in development. Each product is awarded a score of 1-5 in each criterion, the sum of which should decide the overall effectiveness of the product relative to its peers. The criteria for analysis are:

Public Safety and Privacy Protection

This is an essential criterion for our project since the main idea behind designing a predictive anomaly detection algorithm is to protect users from theft and hacking in building systems. BACnet protocol lacks in implementing effective security measures because hackers can access any building automation systems through a public domain. Our goal is to alert the building system of a potential breach without human intervention. Our metrics of comparison will be based on the level of protection each of the products offers a BAN overall. A score of 1 implies that the method is ornamental at best and a score of 5 means that the product is enough to defend against any threat to the system, be it a cyber attack or a physical threat.

Responsiveness

Although anomaly detection methods might prove useful to secure BACnet systems, quick responsive approach to real-time attacks is valuable and of great challenge. The anomaly detection algorithm we are trying to implement has to train with multiple sets of data to recognize anomalous data patterns at a fast enough rate. A delay of just a few minutes might prove fatal to cyber-physical systems, resulting in financial loss. A score of 1 in this metric indicates that the method is too slow to deal with the majority of threats to the system, and the mechanism leaves the system wide open to external access. On the other hand, a score of 5 implies that the system is fast enough to deal with all possible threats and prevent any and all information leaks. Note that since we were unable to test each of the mentioned products first-hand, this criterion is only a rough measure of overall responsiveness based off of test results reported by the creators of the techniques.

Adaptability

Cyber threats are evolving at a very fast rate with many doing so in real time. Due to this, the capability of the security tool to adapt itself to the threats is very relevant in assessing the overall effectiveness of the method. A score of 1 in this implies that the product is fixed and cannot be updated to deal with future or evolving threats. A score of 5 means that the system can evolve with the threats perfectly, and updates very frequently. Similar to the above criterion, Adaptability cannot really be measured without exhaustive first-hand testing. However, this metric serves the objective of comparing the mentioned products loosely based on their descriptions.

Comprehensiveness

This criterion indicates the range of anomalies or threats detected by the technique as a function of the number of uncorrelated network parameters monitored by the detection mechanism. A score of 1 implies very poor range, with the tool only analyzing a single network parameter. 5 indicates an all-encompassing range, with the tool analyzing all possible parameters. Note that

while the number of parameters measured may not accurately indicate the detection range of all devices, the majority of detection techniques can be successfully classified based on this criterion.

Measures for failure

This criterion is a measure of the product's capability to cope with system failures and to support the system in such situations. A score of 5 in this implies that the program has robust fallback and backup routines and can aid in system recovery. On the other hand, a score of 1 indicates the absence of any failsafes or recovery options in the program. A middling score in this regard indicates good failsafe options, but no recovery support.

Economic Threat Mitigation

Security solutions in building automation essentially protect the economy from sudden shocks that may occur from system failures in critical installments like banks and industries, and in critical services like sewage treatment plants, power plants, and to some extent the future smart grid (if the building network is fully exposed to the wider area network). This criterion measures the ability of the BAN security solution to prevent, either directly or indirectly, such shocks to the economy. That is, this is an indication of how useful the tool in consideration is in mitigating threats to the economy resulting from a breach in BANs. Lower scores imply the lack of effectiveness of the system in this regard, and 5, the highest score, indicates that the product is an aegis that can defend the economy from all threats a breach in any BAN could pose.

Global Compatibility

Anomaly Detection in Building Automation Systems are essential to monitor the security of the network system. The algorithm to be implemented must be versatile and cater to all types of components in the building facility. New components that are added to the facility such as lights, and HVAC equipment to name a few must be able to integrate with the anomaly detection software. The main goal of the proposed algorithm is to continually adapt its repository of information and learn new trends in data patterns to perform well during attack situations. Lower scores will imply the lack of compatibility to new data results and hence highlight the limited/ introspective nature of the algorithm. Alternatively, a higher score, close to 5, will prove the versatile and adaptive nature of the algorithm to learn new data patterns and novel anomalous sequences in preparation for when an attack happens.

Benchmarking Tables

I. General comparison:

	Password Protection	**AC2000 Interface**	**Unsupervised Machine Learning methods**	**Timing-based detector**	**Finite-state detector**	**THE driven anomaly detector**	**Our Solution**
Technique used	Access protection using passwords; multi-level access with permissions assigned by the manager	Receive third-party Change-of-Value notifications and monitor all events via the security hub.	Clustering methods, SVM, Random forests	Statistical Attributes of data packets (Mean, Range)	Construct a deterministic finite automaton (DFA). Flag anomalies according to periodicity	Autocorrelation, THE Classification, and Fast Fourier Transform	THE-Driven traffic classification with semi-supervised ML techniques
Accuracy (%)	Not Applicable	Information Not Available	93%	>99%	>99%	~96%	-Can't be measured-
Advantages	Easy to implement, most cost-effective; enough for non-critical systems	User-friendly patented application to configure required BACnet alarm or event outputs.	No requirement of data labeling. Easier, cheaper way to analyze and interpret data	Works both by itself and also through the program scheduler	Very high accuracy and highly sensitive. Able to access the deeper network layers	Detector can be used online.	Online Traffic Classification for better understanding of traffic source Adaptive
Disadvantages	Need to be changed periodically, Easy to leak out to external parties, prone to being hacked	Not open to novel detection mechanisms.	With more data features, algorithm analysis method will change every time Difficult to discern the flow of analysis.	Depends entirely on timing bounds.	Only two statistical parameters measure the anomalies.	Frequency analysis needs to be done manually; not accurate in more dynamic real life situations	Lack of data = less sophisticated algorithm
Limitations	Can be deciphered using brute force cracking technique. Does not implement user alert mechanism after multiple login attempts	Only limited to certain events or alarms that take place.	Impossible to have a 0% false positive rate. Requires the training data to be representative of the network traffic. The model can be overfitted and therefore novel detection may become	Only considers the timing bounds of a data packet. Data packets emerging from human driven activities will not be distinguis	Performance degrades for multi-period traffic patterns - slower traffic patterns increase false positive rate.	Impossible to have a 0% false positive rate. Classifies network traffic into only three different categories.	Impossible to have a 0% false positive rate Works well with more data fed into the system. Unable to introduce third party vendor detection.

			obsolete.	hed			
Standards	Already patented therefore it does comply with BACnet standards defined by NIST	Follows their own AC2000 standards therefore can be considered credible	Complies with ASHRAE's standards of Security Assessment ex: status flags, DoS attacks	Complies with most of ASHRAE's standards from NIST	Complies with most of ASHRAE's standards from NIST	Complies with most of ASHRAE standards by training the model to recognize most of the standard attacks.	The testing model should be able to recognize most of ASHRAE's security assessments defined from the NIST

II. Performance comparison (All scores are ranked from 1-5, with 1 being the least and 5 being best):

	Password Protection	**AC2000 Interface**	**Unsupervised Machine Learning methods**	**Timing-based detector**	**Finite-state detector**	**THE driven Anomaly Detector**	**Our Solution**
Responsiveness	1- Basic form of network protection and no automated capabilities to alert user of breach.	2- Only known threat patterns identified, needs to be manually updated	4 - identifies existing and new anomalies but increases the number of false positives	4- Real time response to threats is very good as this measure's differences in code time bounds	Speed varies according to periodicity of traffic patterns. Multiple traffic patterns mean algorithm slows down.	4- Low latency for detection of most traffic anomalies.	Speed of algorithm depends mainly on the amount of data the algorithm has analyzed.
Adaptability	1-Passwords can be made sophisticated but are only as good as the user's creativity	1- Not easily adaptable to new intrusion detections	5-Does not depend on labelled data and better at detecting new anomalies using SVM and Random Forests methods.	3- Can adapt to multi-periodicity traffic patterns, but additional work needs to be done to achieve good performance. This includes testing on new data patterns.	4- Highly sensitive mode of detection means the algorithm can adapt to subtle changes in data packets.	4- Allows the detection of common types of attacks. Depends on labelled data.	5- Can adapt to new attacks due to unsupervised aspects and also better at identifying threats due to supervised learning methods

Comprehensiveness	1- None because this is a static method of protection.	2- Only known threat patterns identified, needs to be manually updated	4- Responds to a wide range of threats as the method works on identifying the normal pattern and checking for anomalous data packets	3- Only applicable for time driven anomalies.	5- Highly sensitive to all changes in the interface-controller channel, analyzes deeply into the network	4-Trained to recognize different intrusion detection mechanisms through the BAS networks and synthetic generated attacks.	5- Should be able to detect any anomalous data packets due to comprehensive classification of normal traffic
Measures for failure	2- Alerts User regarding breach, ask for change password, lock system operations until authorized.	3- Alert management about successful attacks, infiltrators, and other network data red flags.	1-Non-anomalous data were classified as anomalous - increasing the number of false positives. Model fails if anomalies represent a significant proportion of the traffic. No rectification measures were taken.	1-Difficult to check for failure as some breaches may occur undetected due to limited detection parameters	4- Any anomalies in the channel are found easily due to changes in the DFA of data packets	3 - Methods to alert user can be added to the mechanism. Built-in measures not available.	1- We have not planned any failsafe as of now

III. Macro-level comparison:

	Password Protection	**AC2000 Interface**	**Unsupervised Machine Learning methods**	**Timing-based detector**	**Finite-state detector**	**THE driven anomaly detector**	**Our Solution**
Public safety and privacy protection	Password can be available to anyone	Password can be available to anyone	Password to the main computer used in the experiment	Password for the main computer + Available	Password for the main computer + Available exclusively for facility manager	Password for main computer	Only available to building managers.
Economic Threat Mitigation	This mode of protection doesn't vastly mitigates	This method does not guarantee protection from	Algorithm able to make inferences based on data, but mainly depends on	Scope is extended to time-driven events. Hence	Low false positive rate guarantees lowered economic	Classification of traffic patterns, and frequency analysis	Combination of THE-driven and Semi-Supervised to analyze

	the economic threats. Protection only holds until password is leaked.	common hacking techniques Hence, not effective in mitigation	how algorithm interprets it. Economic threat can be mitigated.	only a part of economic threat mitigated.	threat and fast response to data breaches.	produces an effective way of reducing data intrusion threats.	vast ranges of data to safeguard against any type of attacks. Reduced economic threat due to the versatility of algorithm.
Global Compatibility	Compatible for any systems.	Compatible with most BMS systems	Compatible with BMS systems	Compatible with SCADA systems	Compatible with SCADA systems	Compatible with SCADA and BACnet systems	Compatible with SCADA and BACnet systems

Benchmarking Study Analysis and Summary

After choosing the relevant list of criterias to evaluate our designs, we compared the performance of existing solutions with that of ours.

In our design we plan to use an existing semi-supervised machine learning model because we believe it will reduce the number of false positives as well as the amount of time needed to analyze the network traffic. We have adapted our project from an existing solution that implemented THE-driven classification of network traffic. We include this method because we would like to develop a comprehensive model of BACnet traffic, the individual categories of which can then be correlated with their respective normal patterns. As such, our project has features that are quite similar to the THE-based detector. The difference would be that we use machine learning techniques to label the data rather than frequency analysis. Including ML techniques will improve the responsiveness and adaptability of our proposed design. Automating the process of data capture from network traffic and analyzing for anomalies will allow timely capture of potential intrusions into the system, thereby increasing responsiveness. Semi-supervised ML has the capability of learning from new data patterns in case it fails to detect a new anomaly, thereby improving adaptability.

With regards to responsiveness and failure measures, we do not possess a definite solution since we still haven't designed the algorithm and reached the testing phase. We aim to use one computer to monitor the network traffic and detect anomalies. The limitation we currently have is on the BACnet datasets which we do possess from Qatar University but only for 2 hours. However, if we pursue with the logistical process of obtaining BACnet data from Qatar Foundation under the JBK controls company we will be able to get much more data to train the semi-supervised model.

A pivotal criterion for anomaly detection mechanisms would definitely be privacy protection and economic risk mitigation since these form the backbone of any project. We believe that a strong intrusion detection system would be possible if the attacker has received the password credentials through the BMS system or if they have achieved access through any of the BACnet devices. A robust detection system should classify traffic patterns and continually learn from new datasets using advanced algorithm to guarantee data protection and protect organizations from financial losses. In this regard, our project will aim to fill in the gaps in the security sphere of BACnet infrastructure using the extensive literature review carried out from existing solutions and promote a secure BACnet system.

References

[1] 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]

[2] 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].

[3] 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].

[4] 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.

[5] 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].

[6]"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].

[7]“AC2000,” *AC2000 Access Control & Security Management | CEM Systems*. [Online]. Available: https://www.cemsys.com/products/access-control-systems/ac2000/ . [Accessed: 06-Nov-2019].