CYBERATTACK DETECTION FOR WIRELESS SENSOR NETWORKS WITH DEEP LEARNING

Ulrich Lang, Reza Fatahi, Holmes Chuang
ObjectSecurity LLC

***Abstract* - We present the results of our Navy-sponsored research effort to develop an approach and a working Proof of Concept (PoC), to prove the core hypothesis that our proposed technical approach with Machine Learning (ML) identifies CBM+ networks under cyberattack, and proves a benefit within the given constraints.**

Introduction

Security concerns slow the adoption of wireless predictive maintenance and/or Condition Based Maintenance (CBM+) networks – to detect whether equipment needs to be maintained or repaired. But the technology can be used for many other wireless sensor networks as well, such as industrial control systems or internet of things.

However, CBM+ solutions are currently not focused on cyberattacks but focus on maintenance cases.

Deep learning offers a way to analyze sensor traffic and data to detect cyberattacks – and also to quickly learn sensor network patterns when initially fielded.

Objectives

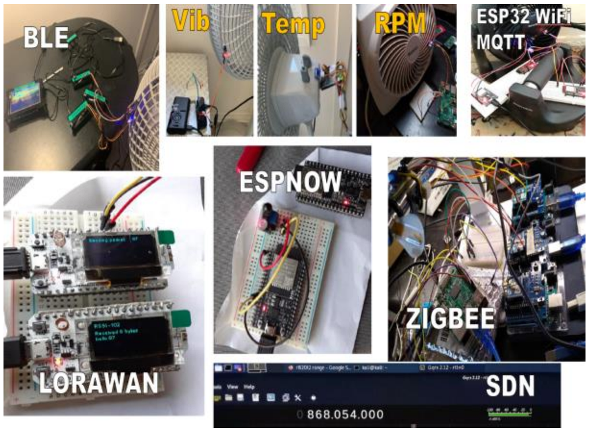
Funded as part Navy STTR N20A-T011-0259 “Cyber Resilience of Condition Based Monitoring Capabilities” we were tasked to develop an approach and a working Proof of Concept (PoC), to prove the core hypothesis that our proposed technical approach with Machine Learning (ML) identifies CBM+ networks under cyberattack, and proves a benefit within the given constraints.

Additionally, ensure that correct sensor data is available at the point of processing – focusing on the analysis of the sensor data, not on the protection of the communication between sensor and a processing unit, or other attacks against sensors and process units.

Also enable organizations to detect and respond to cyberattacks better and faster.

Materials & Methods

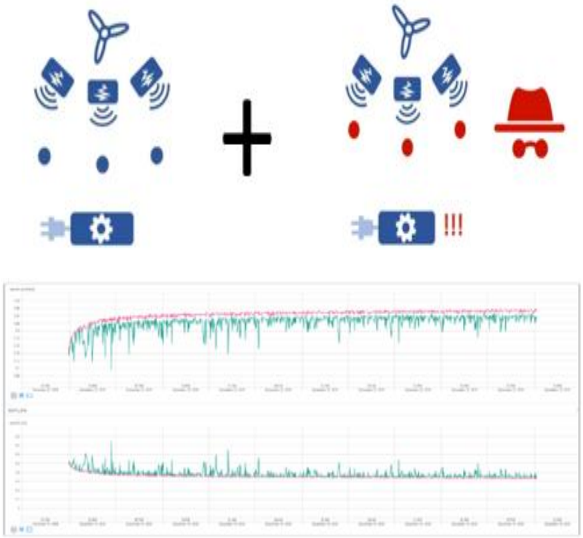
In this 6-month project, we were mainly concerned with proving the core hypothesis, we researched and designed a PoC whose implementation consisted of several wireless sensor network testbeds (Wi-Fi, Zigbee, and Bluetooth) that allowed data to be captured at the gateways – both without and with cyberattacks (esp. denial of service, DoS). In our use case, the sensor network’s gateway, which receives and processes the sensor traffic, analyzes the received sensor traffic on a continuous basis to determine the need for maintenance.



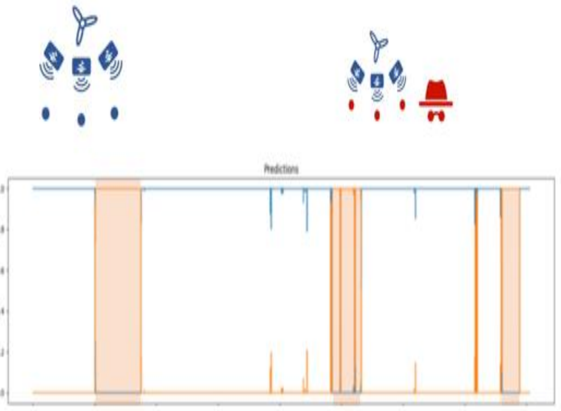
We then successfully implemented working PoC software to analyze the captured data using ML, including time series ML, deep learning ML, and full-fledged CV. During our experimentation, the PoC was able to accurately determine the presence of cyberattacks from data that was not previously seen or trained.

Experimentation

<u>1) Train Deep Neural Network</u> with network traffic data with ongoing cyberattack, and without cyberattack.



2) Experiments automatically analyzes the extracted firmware for known and zero-day vulnerabilities, including binary vulnerabilities



Results

Our preliminary results successfully validate our core hypothesis that the solution with deep learning can identify cyberattacks and benefit CBM+. Particular findings include:

- It is practical to detect cybersecurity attacks from the sensor data using ML.
- Retraining to adapt to new sensor networks can be quick
- A number of attacks (incl. denial of service, DoS) can be detected from traffic packet timings alone,
- It is challenging to mount successful cyberattacks at scale on secured COTS networks to collect data
- A combination of ML approaches appears yield the highest accuracy
- Based on the evolution of ML hardware in recent years (e.g., Nvidia TITAN-V, Jetson Xavier, Snapdragon etc.) we extrapolate that the required processing power will be available in a form factor that can be deployed at s sensor network at the edge

Conclusions

We preliminarily conclude that:

- The approach is viable
- Further research is needed until the technology can be fielded
- Interviews with potential users indicate that there are use cases for this technology

References

- objectsecurity.com/ai
- objectsecurity.com/publist
- https://www.navysbir.com/n20_A/N20A-T011.htm

CYBERATTACK DETECTION FOR WIRELESS SENSOR NETWORKS WITH DEEP LEARNING

Ulrich Lang, Reza Fatahi, Holmes Chuang – ObjectSecurity LLC

INTRODUCTION

Security concerns slow the adoption of wireless predictive maintenance and/or Condition Based Maintenance (CBM+) networks – to detect whether equipment needs to be maintained or repaired. But the technology can be used for many other wireless sensor networks as well, such as industrial control systems or internet of things.

However, CBM+ solutions are currently not focused on cyberattacks but focus on maintenance cases.

Deep learning offers a way to analyze sensor traffic and data to detect cyberattacks – and also to quickly learn sensor network patterns when initially fielded.

OBJECTIVES

Funded as part Navy STTR N20A-T011-0259 "Cyber Resilience of Condition Based Monitoring Capabilities" we were tasked to develop an approach and a working Proof of Concept (PoC), to prove the core hypothesis that our proposed technical approach with Machine Learning (ML) identifies CBM+ networks under cyberattack, and proves a benefit within the given constraints.

Additionally, ensure that correct sensor data is available at the point of processing – focusing on the analysis of the sensor data, not on the protection of the communication between sensor and a processing unit, or other attacks against sensors and process units.

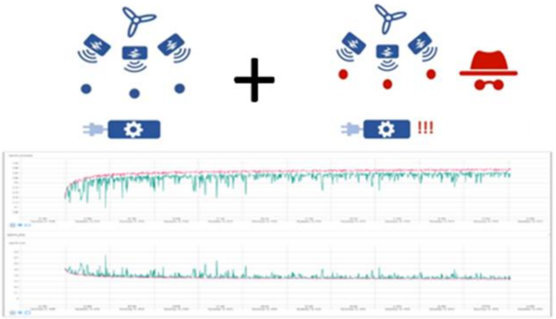
Also enable organizations to detect and respond to cyberattacks better and faster.

MATERIALS & METHODS

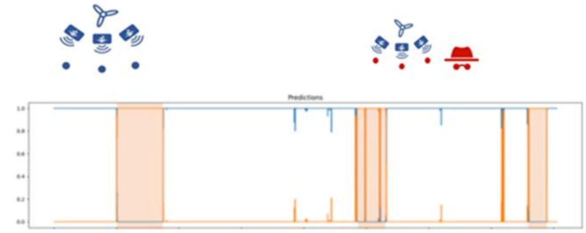
In this 6-month project, we were mainly concerned with proving the core hypothesis, we researched and designed a PoC whose implementation consisted of several wireless sensor network testbeds (Wi-Fi, Zigbee, and Bluetooth) that allowed data to be captured at the gateways – both without and with cyberattacks (esp. denial of service, DoS). In our use case, the sensor network's gateway, which receives and processes the sensor traffic, analyzes the received sensor traffic on a continuous basis to determine the need for maintenance.

We then successfully implemented working PoC software to analyze the captured data using ML, including time series ML, deep learning ML, and full-fledged CV. During our experimentation, the PoC was able to accurately determine the presence of cyberattacks from data that was not previously seen or trained.

1) Train Deep Neural Network with network traffic data with ongoing cyberattack, and without cyberattack.



2) Experiments automatically analyzes the extracted firmware for known and zero-day vulnerabilities, including binary vulnerabilities assessments, decompiling or disassembling and analyzing the decompiled source. Results are aggregated, filtered, mapped to a standard, and prioritized by potential impact



RESULTS

Our preliminary results successfully validate our core hypothesis that the solution with deep learning can identify cyberattacks and benefit CBM+. Particular findings include:

- It is practical to detect cybersecurity attacks from the sensor data using ML.
- Retraining to adapt to new sensor networks can be quick
- A number of attacks (incl. denial of service, DoS) can be detected from traffic packet timings alone,
- It is challenging to mount successful cyberattacks at scale on secured COTS networks to collect data
- A combination of ML approaches appears yield the highest accuracy
- Based on the evolution of ML hardware in recent years (e.g., Nvidia TITAN-V, Jetson Xavier, Snapdragon etc.) we extrapolate that the required processing power will be available in a form factor that can be deployed at s sensor network at the edge

CONCLUSIONS

- The approach is viable
- Further research is needed until the technology can be fielded
- Interviews with potential users indicate that there are use cases for this technology

REFERENCES

- objectsecurity.com/ai
- objectsecurity.com/publist
- https://www.navysbir.com/n20_A/N20A-T011.htm

CONTACT

ObjectSecurity LLC
1855 1st Ave #103, San Diego, CA 92101
info@objectsecurity.com, 650-515-3391,
@objectsecurity

ACKNOWLEDGEMENTS

Parts of this work is sponsored by the Navy under STTR contract [redacted]