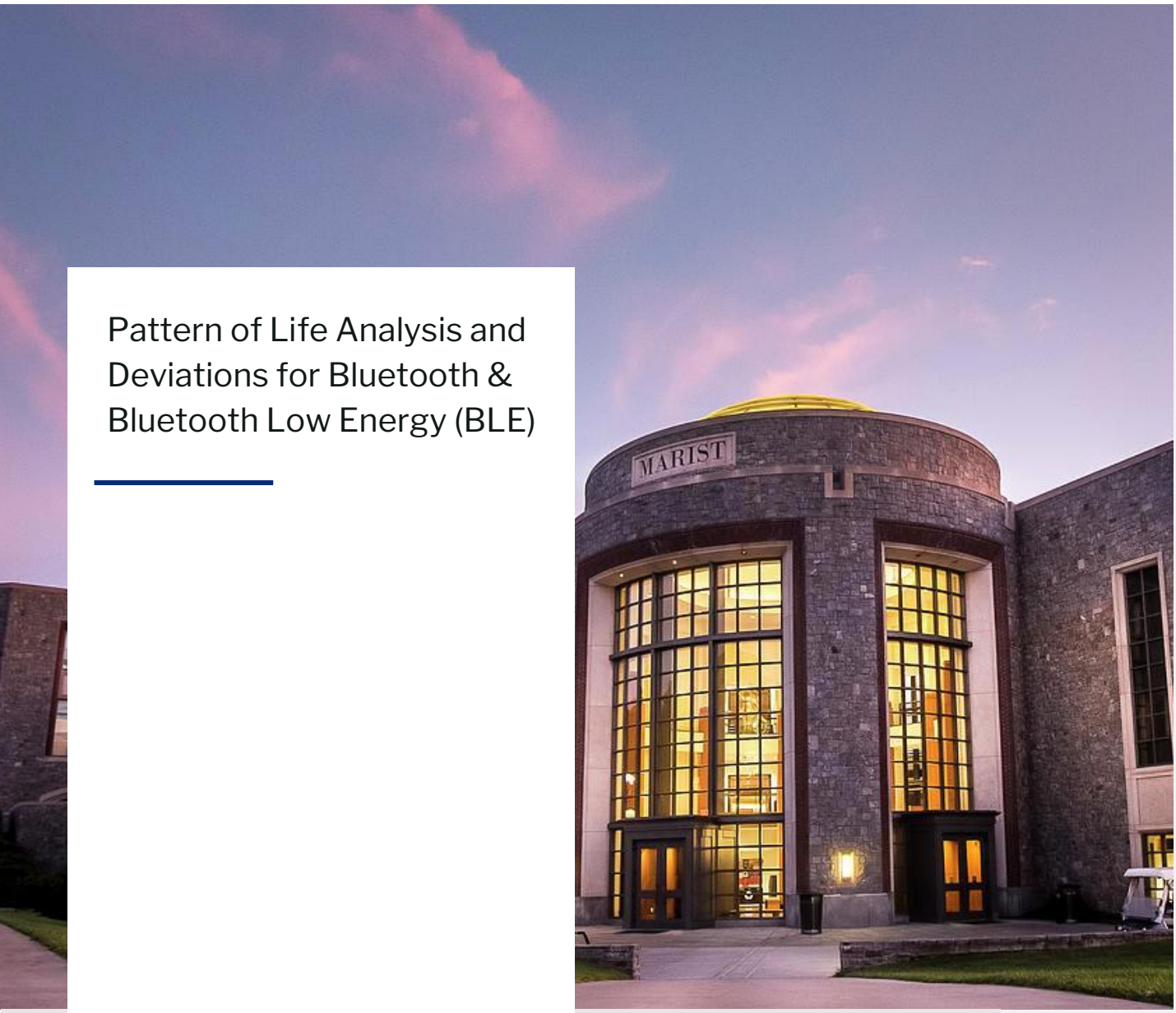

Pattern of Life Analysis and Deviations for Bluetooth & Bluetooth Low Energy (BLE)

APRIL 21

Authored by: Fred Berberich
Sponsored by: Professor Dominick Foti

Research Problem

Bluetooth and Bluetooth low energy (BLE) are short-range wireless technologies that use public non-encrypted advertising channels to announce their presence to other devices[1]. The evolution of smart devices (watches, fitness devices, lighting systems, refrigerators, etc) has tremendously increased the use of BLE communications in a broad range of applications. The millions of deployed BLE devices have drastically increased the rate of cybersecurity threats posed by malicious attackers. Monitoring the communication patterns of BLE devices to ensure that they are behaving appropriately has become increasingly difficult over the past decade. It has become a significant challenge to identify devices using captured traffic produced by Generic Attribute Profiles (GATT) from several Attribute Protocol (ATT). As is documented, detection of BLE devices deviating from the normal operation can provide early warning of measures of possible or ongoing attacks

Interest From Outside Agencies

The National Security Agency (NSA) of the United States identified and proposed a variation the research problem above as part of their participation in the INSuRE Program, a prestigious, high impact learning opportunity for Higher Education Institutions that are accredited as a National Center for Academic Excellence in Cybersecurity. While I will not be directly partnering with the NSA for this project, the research problem is still sourced from challenges identified by them.

Expected Outcomes

Through well-planned evaluation of Bluetooth and Bluetooth Low Energy protocols and behavior patterns, I will deliver my analysis on Bluetooth and BLE devices communication and behavioral patterns, identify how a device advertises itself; what constitutes normal behavior; and any abnormalities in behavioral patterns over the course of the research period. Also, I intend to examine ways in which Machine Learning (ML) could be implemented to detect any deviation in the patterns of Bluetooth devices monitored in our environment. My project will consist of three phases outlined below.

Previous Work

During the Spring of 2023, Professor Dominick Foti instructed an independent study which focused on this exact problem. While progress was made, significant additional work is still needed to advance this area of knowledge. The students in the independent study were able to survey the existing literature that addressed the establishment of patterns of life for Bluetooth devices, implementation of attacks on vulnerable Bluetooth devices, and identification of deviations in network traffic using machine learning and artificial intelligence algorithms. Additionally, the team was able to establish a testbed for both collecting and analyzing Bluetooth Traffic. This research will be used as a foundation for the proposed project.

Phase 1: Data Analysis
Key Deliverables: Data collected from the Bluetooth devices & pattern-of-life (PoL)

Upon choosing devices that will be used to send and receive Bluetooth packets, I will be creating a pattern of life for a Bluetooth/BLE device to demonstrate understanding of the concept, this will include me building

a visualization to show the device's behavior throughout the day. Once this has been successfully completed for one device, I would then repeat these actions for 2-3 more Bluetooth/BLE devices from different categories. This will allow me to start the process of making a pattern-of-life.

Phase 2: Implementation of attacks on Bluetooth
Key Deliverables: (PoL) with the anomalies

After successfully creating a pattern-of-life with the data collected from the interactions between Bluetooth devices, I will then introduce the devices to an anomaly to the Bluetooth devices to create abnormal behaviors. These behaviors may be a technical solution such as SweynTooth or BrakTooth, or a non-technical solution such as repeatedly rebooting the Bluetooth device. I will then generate a pattern-of-life with the anomalies, overlapping with the baseline pattern-of-life, to see if the anomalies can be detected with the features and attributes selected.

Phase 3 – Machine Learning
Key Deliverables: Data collected from which anomalies the ML detects

I will use machine learning (ML) algorithms to be able to detect not only which device is which but more or so focus on when there is an anomaly that is present within a device. I will be able to do so by plugging in Topological data analysis and time series analysis into the machines' algorithms. I acknowledge this will be a challenge since BLE utilizes MAC address randomization and fingerprinting these devices will be difficult.

Academic Benefits

I am motivated to research and gain a better understanding of Bluetooth and Bluetooth Low Energy (BLE) protocols and behaviors. As these technologies become a greater presence in our devices, and thus our lives, it is essential to understand their behavior - the methods, patterns, and contents of their regular communications. We are all affected by the behavior of these devices, regardless of profession or interest in the subject. The fact that relatively little work has been done in this field only serves to increase my interest.

I am looking forward to contributing to the body of knowledge that is accumulating around this subject. The possibility that my efforts can influence the work of others, that I can provide a new foothold to be leveraged on future climbs, is both thrilling and humbling. Another thing that I am excited about is having such a wide impact on not only the Information Technology industry, but everyday life in general. Additional understanding in this field that can be applied to make devices communicate more securely enhance our capability to monitor their communications and identify those that are behaving outside of the norm, is a benefit to everyone.

Through my experiences thus far at Marist College, I currently work in the networking lab helping students who are struggling with Internetworking. Some things we cover are going over different types of networks and protocols that can be used within those networks. I believe conducting research on Bluetooth devices and being able to use machine learning to identify attacks upon those devices is an astounding opportunity for me to use the information that I learned in class and use it to continue my passion towards cybersecurity.

Commented [DF1]: These paragraphs are what we call external motivations. They are great, but what Marist really cares about is that the student gets something out of it. Perhaps a paragraph citing your experience in the Networking lab, and your passion of the intersection of networking and cyber would be great here. Pick one of these paragraphs that you feel is least important and delete it.

Proposed Timeline

The following timeline is proposed to complete the aforementioned Phases of Research:

	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12
Phase 0: Foundations												
Understand prior work												
Recreate Testbed												
Phase 1: Data Analysis												
Data Collection												
Delineate Device Traffic												
Phase 2: Attacks on Bluetooth Devices												
Identify Selected Attacks												
Implement Attack 1												
Implement Attack 2												
Phase 3: Machine Learning to Identify Malicious Traffic												
Dataset Cleaning												
Select ML Algorithms												
Tune Model												