University of Cincinnati

Date: 10/25/2016

I, Pallavi Meharia, hereby submit this original work as part of the requirements for the degree of Doctor of Philosophy in Computer Science & Engineering.

It is entitled:

Secure Trust Establishment in an Internet of Things Framework

Student's name: **Pallavi Meharia**

This work and its defense approved by:

Committee chair: Dharma Agrawal, D.Sc.

Committee member: Raj Bhatnagar, Ph.D.

Committee member: Karen Davis, Ph.D.

Committee member: Chia Han, Ph.D.

Committee member: Erin Nicole Haynes, Dr.P.H.

22332

Secure Trust Establishment in an Internet of Things Framework

by

Pallavi Meharia

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Computer Science and Engineering

in the
Department of Electrical Engineering and Computing Systems
of the
College of Engineering and Applied Science
of the
University of Cincinnati, Cincinnati

Committee:

Professor Dharma Prakash Agrawal, Chair
Professor Raj Bhatnagar
Professor Karen C. Davis
Associate Professor Chia Han
Associate Professor Erin Haynes

October 2016

Abstract

Taking a leaf out of many-a science fiction novels, the future of technology rests upon Internet ubiquity, with wearable technology and intelligent transportation systems leading this revolution. It is projected that by 2020 there will be an approximate 50 billion devices connected to the Internet. This rapidly developing technology is singly responsible for changing the world as we know it, and is popularly coined the "Internet of Things". This research has been undertaken with the goal of providing for a secure framework wherein critical information can be relayed across open communication space, free from interference and intrusion.

In this dissertation, we address security issues in various subunits which jointly contribute towards this heterogeneous network architecture. We introduce a biometric solution geared towards identifying the individual, thus finding a place in home automation environment(s). As part of this work, we are adopting something as mundane as the human walk and transforming that to serve as a critical component of this architecture - the encryption key. For our second subsystem, we address the domain of wearable healthcare technology. Here, we propose two new key management schemes for providing secure link connectivity between the wearable devices and the access point, which too resides upon the host. As a part of this work, we propose to analyze and provide solutions for every communication link in the Wireless Body-Area Network architecture. As our final domain, we target the area of intelligent transportation systems leading to autonomous vehicles. Here, we propose a statistical framework that provides a quantitative score for validating road infrastructure. This methodology aims to mitigate the fears associated with this technology by strengthening the overall decision making skills of the vehicles themselves, such that it learns to recognize good from the bad. The goal is to protect the users by preventing attackers from overtaking the vehicle externally.

This dissertation is novel in its approach and design; varying from suggesting new biometrics for establishing identity, to new architectural framework(s) and techniques for the establishment of a secure communication channel. Given its scope and wide application, the Internet of Things is an emerging area of research. As such, the awareness of and research in this field is important, with security and privacy being a primary concern.

Acknowledgments

It is with great pleasure that I would like to thank every single individual who has made it possible for me to make this dissertation possible and achieve such a milestone in my life. It is difficult to overstate my gratitude to my advisor, Dr. Dharma P. Agrawal. His guidance, enthusiasm, inspiration and support has helped me evolve as an individual. As I sought new paths and oppurtunities, he has always been extremely encouraging. Under his mentorship, I learnt a lot and his devotion towards research and his love for the subject, insprised me to mimic the same. While I could possibly never mirror his level of excellence, I am extremely grateful to have him as my mentor and I will forever remain indebted to him.

I would like to extend my humble gratitude towards my committee members Dr. Raj Bhatnagar, Dr. Karen Davis, Dr. Erin Haynes and Dr. Chia Han for their invaluable advice and feedback on my research and thesis.

To all my past and present peers at CDMC, I am extremely thankful for all those rivetting hours spent discussing and brainstorming ideas, and the light hearted moments that followed afterwards. Thank you for being my family and support system while at UC. I would like to give a special shoutout to ACM-W@UC, every single girl I met there is special and it was a honor to know and interact with them. I hope I could bring some good to your efforts and I hope you all continue the wonderful work you're doing. To all my friends, who are spreadout across the world, thank you for your unwavering friendship and support.

Finally, I would like to mention the tremendous efforts taken by my entire family towards

making me the person I am today. My mother, Veena Meharia, who raised me, loved me and supported my education. My late father, Satish Meharia, who has always watched out for me. I would like to thank my sisters Dr. Priyanka Meharia and Mallika Bansal for being my shields. My brother-in-laws, my nephew and niece, all of whom mean the world to me. I would like to give special appreciation to Dr. Nakul Jindal, for providing emotional support and for including me in your wonderful family.

Lastly, I would like to thank Apple Inc. for providing support during the third year of my Ph.D. and for hosting me for several wonderful internships.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet of Things (IoT) is rapidly paving the way to a wide array of IoT based applications with the goal of simplifying everyday life. Traditional IoT applications range from general household settings and vehicles to more personal forms of computing such as wearables. Research has shown that the technology is of great potential and promises to alter the world as we know it today [1]–[3].

The Internet of Things involves connecting physical objects and endpoint devices to the Internet. Given the wide scope of IoT applications, it has introduced a large number of issues. Restrictions, on the devices and the infrastructure, such as limited memory, processing and computation prowess are affecting wide-scale adoption.

Meanwhile, a number of challenges are affecting IoT adoption numbers. In terms of scalability, IoT applications that require large numbers of devices are often difficult to implement because of the restrictions on time, memory, processing, and energy constraints.

For example, calculation of daily temperature variations around all of the country may require millions of devices and result in unmanageable amount of data. Also, the deployed hardware in IoT often have different operating characteristics, such as sampling rates and error distributions. On the other hands, sensor and actuator components of IoT are very complex. All of these factors contribute to the formation of the heterogeneous network components jointly forming the backbone of IoT; in which the data generated by the IoT devices are of mixed variety. As it is expensive to transmit huge volumes of raw data in the complex and heterogeneous network, so IoT applications need data compression and data fusion to reduce the data volume. Consequently, standardization of data processing methodologies for future IoT applications is highly desired. What is more important is that hackers, malicious software and virus in the communication process might disturb data and information integrity. With the development of IoT technology, information insecurity can directly threaten the entire IoT ecosystem.

Nowadays, IoT is widely adopted in numerous everyday life applications such as smart grid, intelligent transportation, smart health, and smart home. Access cards, bus cards readers and some other smaller applications also belong to IoT. Applications of IoT can bring convenience to people, but if it cannot ensure the security of personal privacy, private information may be leaked at any time. The need of securing communication in IoT devices and applications cannot be ignored. Once the signal of IoT is stolen or compromised, it will directly affect the security of the entire information. With the growing demands of devices connecting to the Internet with more extensive wealth of information, the risk of exposure

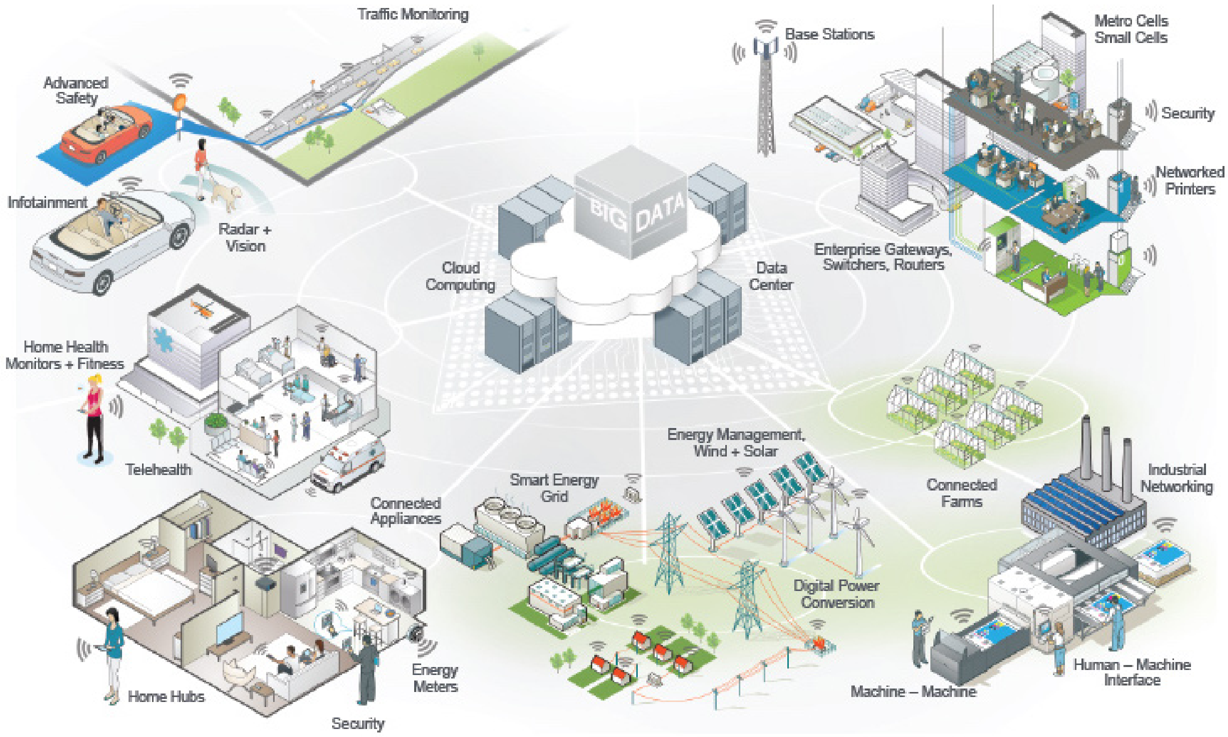

Figure 1.1: Enabling smart connected solutions from the end node to the cloud [4]

of such information also increases. If good solutions for security issues in IoT applications are not present, it will largely restrict its development and adoption. From all of the IoT problems mentioned above ensuring security is particularly important.

1.1 Motivation

Envision a world where Alice wakes up in the morning, and as she dons her slippers and walks across the room, the (smart) house around her wakes up as well. As her home adjusts itself to her preferred settings; we see the different mechanisms coming together into making the home truly Alice's. She goes through the motions of her daily routine as she prepares to head out to work. Her clothes are composed of touch-sensitive textile(s), she has a smart watch on her wrist, health monitoring earphones in place, to name a few possibilities. With her cellphone tucked safely in her pockets, she makes her way towards the front door. As she approaches the door, it senses her coming towards it and unlocks by itself, once she's outside, the house locks up for itself automatically, seamlessly. While all these actions occur, the house informs Alice's car that it needs to now exit the garage and wait for her outside the door. The self-driving car obliges, and as it senses Alice approaching, the car unlocks itself. Once Alice is inside the vehicle and the destination is determined, it drives itself off.

The example above illustrates the possibilities of a smart connected world, which itself is powered by embedded connected devices of various scales and magnitudes. Collectively, they fuel the technology that is IoT. However, given the complexity of all the components which are constantly communicating with one another and the overall heterogeneous nature of the system, there are several vulnerable access points in the network architecture where unlawful entry might be gained by otherwise unauthorized individuals Fig. 1.1. The basic threats of IoT maybe listed under three categories: security, privacy and safety. Ranging from critical infrastructural compromise to possible national and infrastructural espionage. Threats to this technology could possibly affect power, food supply, water, to name a few.

In a much publicized recent hack, researchers successfully hacked two cars and wirelessly controled the brakes, taking the control away from the driver [5]. In another event, a luxury yacht was forced to go off course as researchers hacked the GPS signals that were used for

Physical Attacks	**Network Attacks**	**Software Attacks**	**Encryption Attacks**
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Channel Attacks
RF Interference	RFID Spoofing		Cryptanalysis attacks: a) Known Plaintext Attack b) Ciphertext Only Attack c) Plaintext or Ciphertext Attack
Node Jamming	RFID Cloning	Spyware and Adware	
Malicious Node Injection	RFID Unauthorized Access		
Physical Damage	Sinkhole Attack	Trojan Horse	
Social Engineering	Denial of Service		
Sleep Deprivation Attack	Routing Information Attacks	Malicious Scripts	Man in the Middle Attack
		Denial of Service	
Malicious Code Injection on the Node	Sybil Attacks		

Table 1.1: Categories of IoT Attacks

navigation purposes. Researchers have shown how TV sets and video cameras (including children' monitors) pose privacy concerns. It has been demonstrated that it is possible to tamper wirelessly with electrical equipment including lighting, power and locking controls (doors and windows), and even industrial control systems.

IoT is the bridge that brings together the virtual world and the physical world, making life easier for the Alice's of the world. The same also brings many life-threatening safety issues. A power system hack in a city may not really affect the lives of those who are above the ground, beyond proving to be mere inconvenience. However, the same cannot be said for those trapped underground in the subway systems, in darkness and left feeling helpless.

1.2 Challenges

Given the proposed vision and increasing expectations riding on the success of IoT, security, privacy and trust come to the forefront of the challenges associated with this technology. Several questions come to light, and this dissertation aims to address some of the same. Here, we focus upon three specific challenges:

- How to recognize devices or individuals, and ensure secure authentication?
- How to provide and revoke access to devices or individuals, using automated solutions?
- How to design light-weight solutions which may find a place in the IoT ecosystem?

Perhaps the biggest shortcoming of present security solutions is that they operate at the frequency at which computer programs operate. Which implies that solutions are a product driven by the threat itself. As researchers and developers it is important to remember that security threats will always exist. As technology becomes more advanced and sophisticated, more innovative techniques would be required to circumvent their effects. Using proper security tools such as user authentication mechanisms, data encryption and resilient coding, it may be possible to bolster the security of an IoT environment. With this research, we provide solutions geared towards addressing authentication concerns associated with the IoT subspace. We propose and evaluate a wide array of heterogeneous authentication mechanisms, with the idea of taking into account future security threats and designing lightweight architectural solutions to improve network resilience and establishing trust between the different components (which collectively form a network topology at any instant).

1.3 Contributions

This dissertation provides solutions to different subsystems which coexist in the IoT ecosystem, and how they could be integrated into a working system.

Our first methodology deals with the application of *gait* as a biometric to recognize a person. Here, we describe a wearable device capable of sensing a subject's locomotion and using this information to generate a key to enable authentication, thereby triggering the corresponding access control mechanism(s). We describe how the data may be collected, and the associated hardware which would be required. We empirically highlight upon the feasibility of this technique's ability in recognizing the wearer over time, singular or from amongst a crowd. We also describe how a key could be generated from the biometric template, and how the user's identity could be obscured, thereby providing enhanced user privacy.

The second methodology talks about a system architecture to secure communication between on-body sensors and the local access point (or coordinator). We present two architectures to achieve the same, one uses multivariate polynomials to secure the communication channels and the other employs a Merkle tree based approach to enable the same. Here, we built a simulation model to emulate a full range of human movements, and to evaluate how connectivity is affected by motion. Essentially, we evaluated the performance of the proposed systems against the same simulator.

The final methodology is geared towards addressing securing vehicular mapping needs for autonomous driving. This research proposes a machine learning based system to authenticate road-side fixtures to aid intelligent vehicles. The goal is to provide a scoring system to recognize the legitimacy of road-side fixtures, to prevent attacks such as carjacking. In addition to security, the system also serves to apply crowd-sourced information to enable the smoother deployment of autonomous vehicles alongside legacy vehicles, amongst other possible applications. We provide an analysis of the proposed system using sample data collected from diving a vehicle on a fixed route in the city of Cincinnati.

1.4 Outline

This dissertation is organized according to subsystem from the global IoT ecosystem. Chapter 2 describes the overall language behind the terminology being used in this dissertation and the background behind each subsystem. Chapter 3 proposes and evaluates the use of gait as a biometric. Chapters 4 and 5 deal with securing communication in a Wireless Body Area Network, paving a way towards designing more secure medical sensor networks. Chapter 6 describes a scoring system for road-side fixtures to prevent carjacking for autonomous vehicles. Finally, Chapter 7 serves as the conclusion where we address future enhancements and possible solutions towards fortifying the IoT ecosystem.

The

Chapter 2

Background and Preliminaries

While the vision for IoT started out with heavy focus on the nature of things that were connected (such as sensors or RFID's), focus is now gradually moving towards controllers and actuators as being prime representative of *Things* in IoT. This technology gives more weight on being interconnected and diverse, encompassing a wider range of devices which communicate on the same platform, more so than previous iterations of the Internet. Simply put, this technology refers to *the entity is active, digital, networked, can operate autonomously to some extent, is reconfigurable and has local control of the resources it needs such as energy, data storage, etc* [6].

Currently, not everything in the physical world is wired to be a part of the Internet (e.g. a table or a chair), but what is to be remembered is that it could be. Given different needs of the IoT space, designing a one-fit all solution is not the most practical approach towards addressing underlying vulnerabilities of this ecosystem. Hybrid identity schemes are needed to meet the demands of the wide range of Things which collectively form the IoT space.

IoT Layer	**Counter Attacks for All Layers**
Physical Layer	**1) Risk Assessment** a) Locating New Threats b) Applying Patches c) Applying Updates d) Providing Improvements e) Upgrading Systems **2) Intrusion Detection Mechanisms specific to IoT Systems** **3) Securing the IoT Premises** a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personnel **4) Trust Management** a) Trust relation between layers b) Trust of Security and Privacy at each layer c) Trust between IoT and User
Network Layer	
Application Layer	

Table 2.1: Security Countermeasures

2.1 IoT Applications

- **Urban Road Transport and Smart Cities**: Such a network consists of smart embedded devices and could be used in applications such as environmental sensory devices, devices embedded in the urban infrastructure, etc. These could range from traffic cameras, traffic light sensors, devices such as a SatNav in a vehicle or even smartphones. In this case, the access points are usually wired to the environmental sensors.

- **The Physical Environment**: Such a network refers to smart devices which are integrated into the physical world, ranging from SatNav's used to detect vehicles to smartphones carried on the human form. In contrast to Urban Road Transport, this environment consists of sensor devices which communicate over a wireless network to an access node.

- **The Human Body**: This type of network consists of sensors worn on the body and collectively form a wireless body area network (WBAN). Here, each sensor device is typically within the range of a mobile hub which acts as the access node to this architecture.

2.2 Wireless Body Area Networks

It is envisioned that the future wearable devices will become common commodities, inter-operating with other smart devices in the vicinity. A person could wear several sensors of different magnitudes and scale, serving different roles of varying medical benefits. The physiological requirements mandate that the sensors to be located at different points of the body, enabling communication between the sensors and other devices using wireless media. A central hub (sink/coordinator) will function as an aggregator, consolidating the readings from other sensors and forwarding the same to the host station. Wireless Body-Area Networks have been studied by multiple researchers, under multiple names (personal area-networks and body-area sensor networks) [7], [8]. The Institute of Electrical and Electronics Engineers (IEEE) 802.15 task group six define a Body-Area Network (BAN) as “a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics/personal entertainment and others”. For our purposes, we assume that the physical layer, the medium access control and the network layers are configured to optimum performance as we are mainly concerned with providing security mechanism for the wireless variant of BANs.

Security Challenges in WBAN

Transmission of medical health information amongst sensors in a WBAN need to satisfy the following security requirements: data confidentiality, data authenticity, data integrity and data freshness. Data confidentiality refers to the hiding of data using a secret key before it is forwarded, and can be done both symmetrically and asymmetrically. This ensures that the data can be read only by the authorized individuals, thereby ensuring privacy. Data authenticity refers to the validation of the sender information to confirm the source of the data. Data integrity verifies that the received content is the same as the original message and has not been tampered with. Data freshness is a check to certify the data content as recent, and prevents system disruption due to the replaying of old messages. There are many security issues associated with wireless sensor networks/ body sensor networks/ body-area networks. Some of them have been identified as [9]:

- **Compromise of Sensor Node(s)**: This security refers to hacking of a deployed sensor. This can include attack, capture and reconfiguration of a sensor node. Having acquired few nodes, the attacker goes onto launch a variety of attacks which include and is not limited to falsification of sensor data, rerouting the traversal path, setting up infinite traversal paths to exhaust the network and extraction of secure information.

- **Eavesdropping**: The attacker is capable of monitoring the transmissions, thereby having access to the communication between sensor nodes and what was initially intended as secure information.

- **Denial-of-Service (DOS) attacks**: By invoking DoS, network topology and functionality can be destroyed. The nature of the DoS attacks are wide-scaled and diverse, rendering them difficult to defend.

- **Malicious use of commodity networks**: Long term application of sensor networks can be extended to usage of the same topology by untrustworthy users. With widespread use, the cost and availability barriers that discourage such attacks will drop, causing an influx of attacks and increase in vulnerability.

The attack itself can be sourced from different sides, with the possibility of the attacks being equally likely originating from the patients side and the caregivers side. Security mechanisms adopted for WSNs (Wireless Sensor Network) do not always provide the best solution for use in a WBAN. The restricted and specific features of WBAN limit the system architecture. WBANs are associated with fewer sensors and with limited communication range. Additionally, given the placement of the sensors on/inside the human body, physical attacks to the system are virtually scarce. Designing security mechanisms for WBAN mandates that all these restrictions be taken into account. Here, key management is an integral component that provides support to secured system architecture.

Security Goals

The purpose of our proposed system architecture(s) is to enable users with devices equipped with sensors that will collect data about their well being and their environment, and relay this information to a service provider for further analysis. In general, an adversary seeks to infiltrate this process and compromise the sensitive data being communicated. As such, our proposed system seeks to achieve the following end goals:

- The proposed system should preserve and protect the confidentiality of the generated physiological data and meta data. This implies that the acquired data should not be made available to anyone but the user and the service provider.

- The proposed system should be designed such that it maintains the integrity of the data being acquired. This implies that the service provider and the user should be able to trust that the data exchanged by them remains unchanged.

- The proposed system should be able to authenticate source of the sensed data and the meta data. That is, the service provider should be able to trust that the sensed data was received from a given user with a specific sensor device.
- The proposed system should obfuscate the sensors itself, implying that the sensors being worn by the individual should be known only to the user and the service provider.

Key Management

Establishing secure communication channels between network devices and sensors is a growing concern. Several research projects have already addressed this issue of formulating a protected technique for key generation and distribution.

Key Pre-distribution in WBAN

A probabilistic key management has been proposed for pairwise key establishment in [10], [11]. The main theme is to establish a common pool which would store all the keys and the sensors nodes randomly select a set of keys. It has been established that any two sensor nodes must satisfy a certain probabilistic key pre-distribution scheme. This idea has been extended and a two-key pre-distribution technique has been proposed. TinySec is a security architecture [12], deployed at the link layer for wireless sensor networks. It has been conceived as a solution to provide security and encryption of biomedical information. Here, a group-shared key encrypts the data packets; the keys are shared between the sensor nodes. The secure packets are generated by computing a MAC (using the key) for the whole packet (including the header). By default, TinySec allocates a single key to each sensor before being deployed. This architecture fails in that by acquiring the data from any one sensor, the entire network data can be determined. Thus the system can provide limited security for it does not provide protection against a node capture. By bypassing the TinySec architecture, the attacker can gain access to both the information at the nodes and can correspondingly feed the nodes with their own information. TinySec has been proposed as a security solution in BANs, and achieves link-layer encryption and data authentication. In the context of secure sensor association, researchers have studied an architecture where each sensor node is associated with a controller using a public key authentication. Here, the user compares the blinking patterns generated by LEDs to verify the associations; it assumes the existence of a trusted authority (TA) for key processing and distribution and does not support batch processing. Message in a bottle [13] and Kalwen [14] employ a faraday-cage where keys are pre-distributed in the secure channel and made available to the sensors before deployment. The security mechanism behind this approach is that no users outside the cage has access to the information contained within, rendering it secure from unauthorized access. The drawback to this is extraneous overhead with respect to the cost and associated equipment.

Hybrid Key Generation

A hybrid key management technique has been proposed which is an amalgamation of pre-distribution of keys and biometric key generation. Here, some of the sensors are preloaded with keys; additionally keys are generated from physiological values [15]. This technique offers plug and play capabilities, and accounts for randomness and reduces system overhead (by eliminating the need for servers and key distribution) [16]. Due to its reduced energy consumption capabilities, it is highly adaptable in a heterogeneous sensor network and in biomedical devices. To achieve this, a local binary pattern (LBP) has been used for feature generation from electrocardiogram (EKG) signals [17].

2.3 Automotive Technology

It is interesting to note that recently Uber launched it's self driving ride-sharing services in the city of Pittsburgh, Pennsylvania. As predicted, autonomous vehicles will soon coexist alongside more legacy vehicles as they start sharing our roads, be it private or commercial. Advances in the transportation industry dates itself as far as the 19th century with the rise of the railroad system. Society has adapted itself around this technology as it transitioned from horses and carriages to this form of locomotion. However even today, when a dog runs onto a train track and is unfortunately run over, no one blames the train. This is simply because we have accepted the train for how it is and that it is simply doing what is its inherent nature. This means, we have conditioned ourselves to live alongside this infrastructure, and become acclimatized to having self-driving cars around us.

Autonomous Vehicle Challenges

Designing solutions for self-driving cars or intelligent vehicles are plagued by multiple hurdles, all of which affect the overall adoption rate for this technology. It is important to understand some of the challenges which are affecting progress:

- **High Precision Map(s)**: (Also known as High Definition maps) They are critical to the success of autonomous driving systems. These maps provide infrastructural and navigation information to the vehicles, and are in supplement to the on-board sensors and cameras. They prove to be especially useful when a vehicle enters a new territory, with little to no information about the surroundings.

- **Lack of Legislative Laws**: Ethically moral dilemmas have ridden this technology ever since its conception and there is a distinct lack of judicial bylaws which dictate its functioning.

- **Security**: This is one of the biggest concerns with this technology and recent research supports this claim. This technology is susceptible to various kinds of vulnerabilities, ranging from physical to software to even hardware compromise. Communication is required to be encrypted and all fingerprints obfuscated. Quick, light-weight and keyless systems are the order of the day, which aim to protect vehicles from both external attackers and malicious roadside units.

- **Heterogeneous Transportation Network**: The complex road network makes it difficult to design one global solution which could cater to every need. At any time of the day, roads consist of cars, bikes, pedestrians and maybe even animals, rendering the whole network to be very complicated.

Attacks on Autonomous Vehicles

There are two broad categories under which vehicular security may be categorized: direct and remote. In general, vehicular compromise refers to attacks on the Electronic Control Units (ECUs) which by itself are based on the Controller Area Network (CAN) standard [18]. Vehicular communication is a product of the communication between these ECU's, thereby securing this communication stack is critical.

Direct Physical Access

As seen in Figure 2.1, CAN packets contain critical information such as housing the identifier and data. By itself, the CAN standard is open for compromise from external attacks.

Some of the ways this have been achieved are:

- Radio: Researchers have shown how the radio on a vehicle may be controlled externally,
- Brakes: A group of researchers demonstrated how the brakes on a vehicle may be controlled externally, preventing the user of braking,

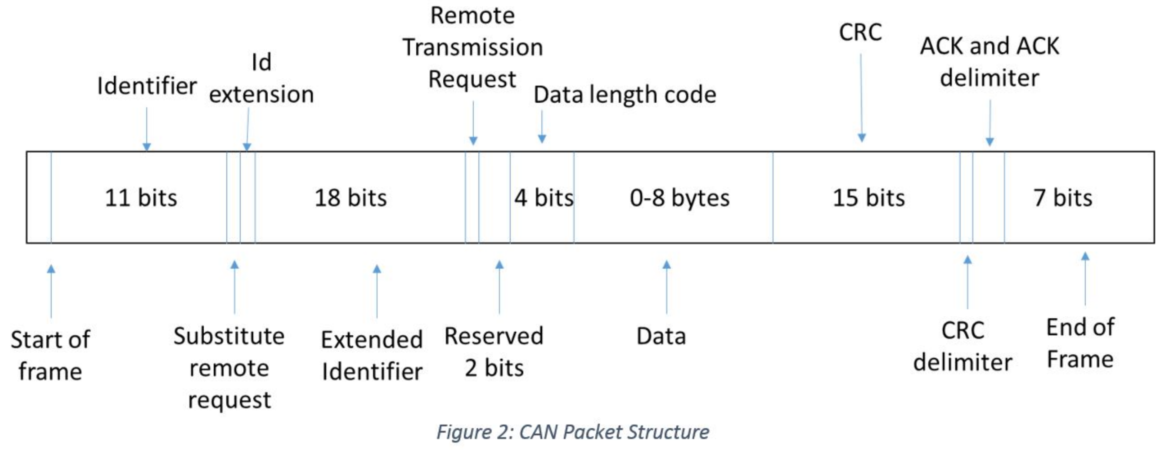

Figure 2.1: CAN Packet Structure

- Engine: Disabling power steering, increasing the RPM or killing the engine of the car as a whole; researchers have shown that they could remotely disable full functioning of a vehicle,

- Instrumentation Panel: Amongst other things, it is possible to provide false information to the driver. This may include incorrect speedometer values, false fuel levels or false error messages.

Indirect Physical Access

This refers to giving access to attackers using external devices, such as a media device (CD) or a PassThru device. Researchers have shown how media tracks on a CD may be modified such that on a regular (PC) audio player, it plays back as expected but on the media player on the car, it sends specific CAN packets to the vehicle [19]. PassThru devices

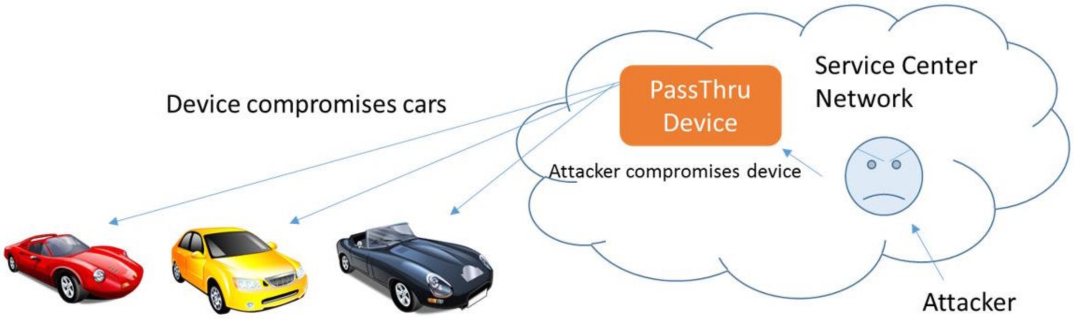

Figure 2.2: PassThru Attack

connect to the OCD-II port on cars and provides access to the internal network of the vehicle. Researchers have shown how the CAN bus may be modified by gaining access by means of the PassThru, including injecting malware.

Short-range Wireless Access

Bluetooth is a major component of infotainment systems in modern day telematics units. However, researchers have successfully reverse engineered the same to render it vulnerable. As shown in Figure 2.3, indirect access may be possible by using the smartphone as an access point. By infecting the user's phone by means of a Trojan, it may be possible to compromise the vehicle. Direct short-range wireless attacks would involve knowing the device' Bluetooth MAC address and brute forcing the PIN which would be required to establish connection.

Long-range Wireless Access

Modern day vehicles come equipped with telematics units capable of providing long-range communication. For example, in the event that a vehicle has a fatal crash, by default it can

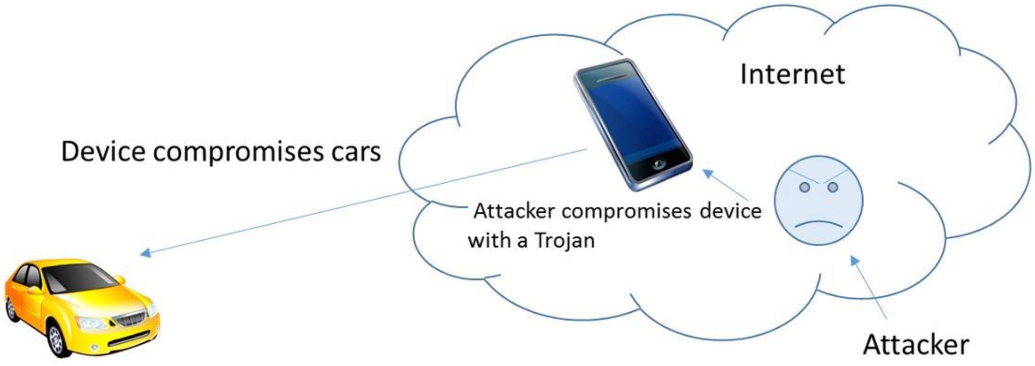

Figure 2.3: Android Trojan Indirect Attack

automatically notify the necessary authorities of the same. However, by exploiting the buffer overflow vulnerability, researchers have shown how it is possible to bypass authentication and force the vehicle to download and execute malicious code. In another experiment, attackers have shown how it is possible to compromise a car by encoding an audio file. In this case, when a call is placed to the car, said song is played back via the on-board microphone, causing the malicious code to be executed.

Security Goals

There are certain key components which should be taken into consideration when designing security solutions for the future automotive technology.

Safety By Design

Security is often an afterthought, wherein issues are addressed and patches are suggested after vulnerabilities and breaches have been found. However, with the advancements being made in technology at large, designers and architects should consider the consequences as an integral part of the requirement phase for the system design. Automakers should take into account all possible moves with the aim of minimizing surface attacks.

Evidence Capture

It is imperative that data be collected from all failure events, such that the same may be incorporated towards the design of future system. However, this would require logging systems to be in place, such as black boxes on airplanes. Automobile manufactures should considering installing similar systems to learn from events and utilize that knowledge in preventing similar future events from re-occurring.

Security Updates

As with any other consumer electronics product, it is important to provide for mechanisms wherein security patches could be sent to devices at a later time. The same should be secure and encrypted and to prevent the patch itself from becoming the target of attacks. To built a secure infrastructure, automobiles are required to be updated in a quick and secure manner.

Collaboration

To promote the design of an effective security infrastructure, it is advisable to have automakers maintain more transparency in their work. This would require them to collaborate their efforts in finding risks and vulnerabilities in security systems. This would also minimize redundant efforts and increase overall productivity and strength of potential solutions.

Chapter 3

Gait Recognition: On-demand Secure Connectivity

Human psyche works such that we learn to identify individuals based on properties we perceive as being distinct about each person, such as face, features, fingerprints, etc. These traits that may collectively or individually distinguish individuals are known as biometrics [20]. With rapid evolutions in technology, it is now possible to design authentication mechanisms for providing access controls systems using biometric recognition as the backbone.

Chapter is based on *"The Human Key: Identification and Authentication in Wearable Devices Using Gait,"* published in *Journal of Information Privacy and Security*, 2015.

3.1 Introduction

A fundamental problem surrounding WBANs is determining who is wearing mobile and sensor nodes. This allows us to recognise the wearer of the device(s) and actuate controls based on the identity. For example, from an infotainment perspective, by recognising the person wearing the devices, the preferred game mode or music may be triggered to auto-play. From a home automation perspective, we can adjust the home controls to the user's preferred settings based on the identity. We can trigger doors to lock and/or unlock based on the identity. One such compelling use-case is to identify a user such that his/her correct identity is associated with the corresponding health records.

This problem that deals with recognizing persons based on their physiological characteristics is a well established field. This chapter deals with a methodology that does the same using simple, non-invasive, inexpensive hardware; all in real-time. Here, we present a biometric system which applies wearable sensors to collect identifying information about the wearer. Then, a model of the biometric is used to identify the user in later events, after which it should be able to do independently and unobtrusively.

3.2 Biometrics

Biometrics refers to metrics that could directly relate with human characteristics. They are used to recognize, label and describe individuals. In this section, we will address what makes a biometric, various kinds of biometrics and how the same may be used a enable user recognition and authentication.

Characteristics

A good biometric is defined as the one which captures several characteristics, that could collectively complement strength of the feature. A good biometric is one which has the following properties:

- Measurability: A characteristic is measurable when an instance of it may be captured by a device, for example a sensor that is capable of capturing information for post-processing,

- Universality: A characteristic is defined as being universal when it is exhibited by most people, making it relatively widely available,

- Uniqueness: A characteristic must be unique for a given population,

- Permanence: A characteristic is define as being permanent when its value does not vary widely over a relevant time frame,

- Performance: It implies that it should be possible to record the biometric unobtrusively, while ensuring an overall acceptable success rate (less noise),

- Circumvention: A good biometric is one which is challenging to circumvent, and

- Acceptability: For a characteristic to be acceptable, the general population should be willing to both use the device required to capture the information and give permission to use the information for recognition purposes.

Ideally a good characteristic is the one which is easy to collect or scan, preferable with inexpensive equipment and minimum infrastructural costs. It is imperative that data be collected immediately by means of simple, automated solutions.

Categorization

Based on different recognition techniques which have now become common and given the nature of the underlying modalities, two basic categories of biometrics have been identified: physiological (passive) and behavioural (active). A behavioural biometric is one which requires active participation from subjects, i.e., participants need to proactively initiate recognition. A physiological biometric is the one where data collection is more passive in nature and does not require the user to take any decisive action. From a user's perspective, a passive biometric is desirable as its implementation is seamless and unobtrusive. With respect to potential applications, both biometrics exhibit vast differences, directly affecting its overall applicability. Additionally, the method required to collect the data itself affects the overall system design. For example, some systems would require the subject to have a particular sensor attached to them, while another would require the user to proactively interact with a sensor.

It is important to remember that the aforementioned categories are not mutually exclusive. Voice recognition is one such system which exhibits properties from both the categories. While the voice itself is a function of the vocal tract, the tone is also affected by the behaviour. A user's present state of mind may cause the voice to change or adjust depending on mood. To design an efficient biometric authentication system, it is imperative to select the appropriate biometric, which is dependent on the application requirements. A summary of some of these characters is described next:

- Deoxyribonucleic Acid (DNA): It is a molecule that contains biological instructions of the living organisms,

- Ear: The topology of the ear has been determined to be proportional and distinct across a population,

- Face: Facial recognition is widely popular and accepted as a valid solution to perform biometric authentication,

- Fingerprint: Given their individuality and persistence, fingerprints are regarded as one of the most reliable biometric characteristics,

- Gait: This is an emergent behavioral feature which aims to authenticate individuals by the way they walk. This technique exhibits unobtrusive properties, facilitated by the fact that individuals can be authenticated across large distances without requiring active human participation,

- Iris: Similar to fingerprinting technology, iris information is unique and does not change over time,
- Keystroke: This biometric relates to how users type on keyboards. By using interkey times and quantifying overall keyboard interactions, it is possible to characterize individuals,
- Signature: The use of signatures has been been widely spreadout across different areas ranging from legal uses to government documents, and
- Voice: As mentioned before this is a combination of physical and behavioral attributes which are related to an individuals voice signal patterns. This is distributed into two major groups: text-dependent and text-independent methods. In one the user is required to repeat a fixed speech (text) to enable authentication, whereas in the other, no constraint upon the texts are placed.

Table 3.1: Viability of popular Biometrics

Characteristics	Capture	Invariance	Singularity	Acceptance
Two Finger Geometry	Optical (IR)	Good	1: 1000	Very Good
Hand Geometry	Optical (IR)	Good	1: 1000	Very Good
Retina	Optical	Very Good	1: 1 Million	Not Good
Iris	Optical	Very Good	1: 6 Million	Good
Veins of hand	Optical (IR)	Good	Unknown	Very Good
Signature	Dynamic (pressure)	Not Good	1: 10000	Very Good
Voice	Electroacoustical	Not Good	1: 10000	Good
Face	Optical or IR	Good	Unknown	Good
Fingerprint	Optical, capacitive etc.	Very Good	1: 1 Million	Good

Recognition

Biometrics are practical and useful because they enable design of a system which can recognize a person from a given population. Population size is an important parameter directly affecting the performance of the biometric (Table 3.1). For a given population, biometrics may be applied in either of the two ways: identification and verification.

Identification

This is an one-to-many mapping technique that is applied to identify a single individual from a large population. Using a combination of different features, a template is created for a user. This template is used to match the users sample against those collected from the population.

Verification

This is an one-to-one technique applied to verify the claimed identity of an individual against a copy of their template as stored on record. In this case, the biometric recognition function should work such that it proactively rejects the remaining population and only meets the conditions as specified by the subjects biometric.

3.3 Security Challenges

The traditional biometric approaches make use of distinct physiological characteristics of a person, and use the same to determine their identity. This entire process is termed as biometric authentication [20]. The most conventional parameters involve physiological characteristics ranging from non-invasive features such as facial and hand geometry to invasive techniques such as impression from a page finger, distinction of an iris, or structure of the DNA. Some behavioral patterns also page find application in identity association such as voice modulation and acoustics, the mechanics of locomotion, keystroke dynamics [21] and one's penmanship. In general, biometric parameters are qualified by: Invariance, Measurability, Singularity, Acceptance, Reducibility, Reliability and Privacy. Given such considerations, the number of such parameters which posses few applicability, as illustrated in Table 3.1. A point to be taken into consideration is that biometric systems are not perfect nor are they designed to be so; additionally there are two errors metrics commonly associated with biometrics: FAR (False Accept Rate) and FRR (False Reject Rate) [22]. FAR refers to the probability of generating a false positive, which is wrongly identifying and accepting an impostor for a genuine user. FRR refers to the probability of mistakenly rejecting a valid user. These two parameters jointly serve as tools which can gauge the overall performance of a biometric feature in action. A third parameter at which the false rejection rate and the false acceptance rate are equal, also acts as a metric for determining the accuracy of a biometric system known as equal error rate (or crossover error rate (CER)).

3.4 Related Work

Gait analysis is based on a long founded science, dating as far back as the 17^{th} century [23]. Over the years several researchers have concluded that the study of a person's gait is adequate to determine their gender and identity. Most of the research in the analysis of gait has been limited to the usage of photography and video capturing devices, limiting the study to spatio-temporal components. Gait recognition techniques can be broadly classified into three categories: (a) Machine Vision (MV) based, (b) Floor Sensor (FS) based, and (c) Wearable Sensor (WS) based.

MV based gait analysis techniques usually incorporate studying the silhouette of a person as capture on the reel. Usually, the parameters of interest are stride, cadence, height, proportions of bodily features and the overall silhouette of the person [24]–[27]. Cameras used for studies could be video or infrared or a combination of the two, depending upon their use. The main idea behind this monitoring model is to break movement down into a collection of joints and their functioning, thus computing the angular motion of each component during motion. Success has been achieved with recognition rates as high as 95% being achievede results generated are promising with an approximated 95% recognition rate [28], [29]

To compute the kinetrics of gait patterns, FS based monitoring techniques is an excellent application. These involve placement of floor-mounted load transducers, commonly referred to as force sensors. Such a platform is responsible for measuring the ground reaction forces along with the direction, magnitude and location of the applied pressure [30], [31]. Positive success rates of 93% has been achieved using such a technique, with toe to heel time between steps yielding a recognition rate of 80% [31]. While this technique does satisfy the properties that make a good biometric measure, the infrastructure costs involved render this technique economically unfeasible, thus preventing it this application from being aopted in real life. WS based techniques usually involve the usage of inertial sensors such as accelerometers and gyroscopes [32]–[37]. Researchers have also used wearable light sources to study the human form while in motion [38]. The purpose of this technique is to apply the motion sequence generated by the lights in identifing the wearer. WS based identification technique enables the possibility of generating a wide set of parameters for identification purposes, thus providing a large scope for biometric applications. Researchers have also applied using the sensors within a smartphone to study motion and it's repeatability [39], thus proving it to be a candidate for biometric applications.

3.5 Feasibility Analysis

The dataset is analyzed by employing statistical measures for purposes of precisely establishing characteristics in terms of consistency and uniqueness.

Data Distribution

Based on available data, distribution of the stride interval values for (a) a user and (b) across multiple users, have to be determined. This has to be done before establishing its sufficiently generic performance. In the former case, the stride interval generated by each user follows a normal distribution (Figure 3.1). This implies that a particular user tends to follow a rhythmic motion, and each step is almost equally spaced apart, following a normal distribution. Theoretically, the probability density function is given by:

$$f(x) = \frac{1}{\sigma\sqrt{2\Pi}} \exp^{-\frac{(x-\mu)^2}{2\sigma^2}}, \tag{3.1}$$

Where the parameter μ is the expectation value against the sensed data, σ refers to the standard deviation about the mean. It can be concluded that humans in motion tend to adopt a two-dimensional Gaussian distribution. As seen (Figure 3.2), a Gaussian density function is made available at each data point, and over the range of the data, the sum of density functions is computed. Considering the randomness of the sensed data, data from different users exhibits a bell-curve distribution, with the trend for each user being localized around a mean. With every user in consideration, the distribution plot is drawn and a normal distribution can be obtained (Figure 3.2). Although the distribution function for each group is not uniform, the three means for each user is largely centric about a similar mean. The *stride interval* exhibits long-range power-law correlations which indicate a fractal process [40].

Linear Regression Analysis

Before stride characteristics can be accepted as a valid biometric, it is important to establish its consistency and tendency to repeat itself over an extended period of time. Primary

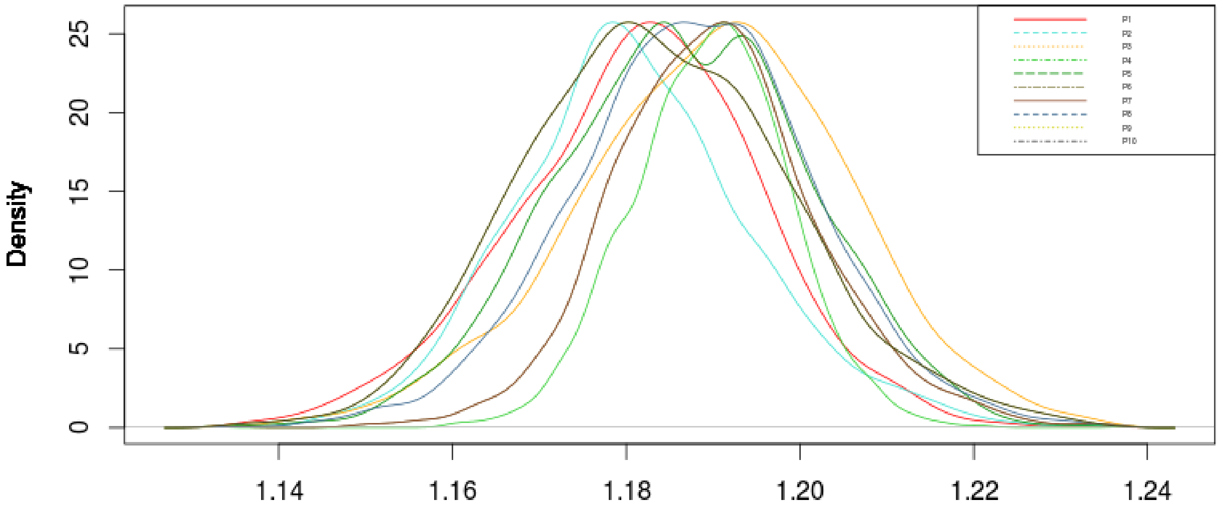

Figure 3.1: Demonstration of Density Estimation

model assumptions that we make when we apply gait as a biometric is that each recorded value can be modelled as a normal random variable assuming, that each occurrence of a statistic is statistically independent and each result obtained traces back to a population having the same variance. To verify the assumptions claimed, plots of residuals have been examined (Figure 3.3). To facilitate generalization, a linear regression model was the adopted tool of choice. A linear model function has been superimposed between a pair of values for a user (pairing made from 2 values from the available set of 3). To perform the summary analysis, a one-way ANOVA (Analysis of Variance) was carried out with alpha > 0.05, exhibiting statistical significance. Our findings determined that normal probability of the plot of residuals are almost identical to the line y=x, inferring that the original data follows a normal trend. Additionally, the plot of the residuals versus treatment (fitted values) implies a constant variance. The results from the ANOVA run are very promising and confirms the

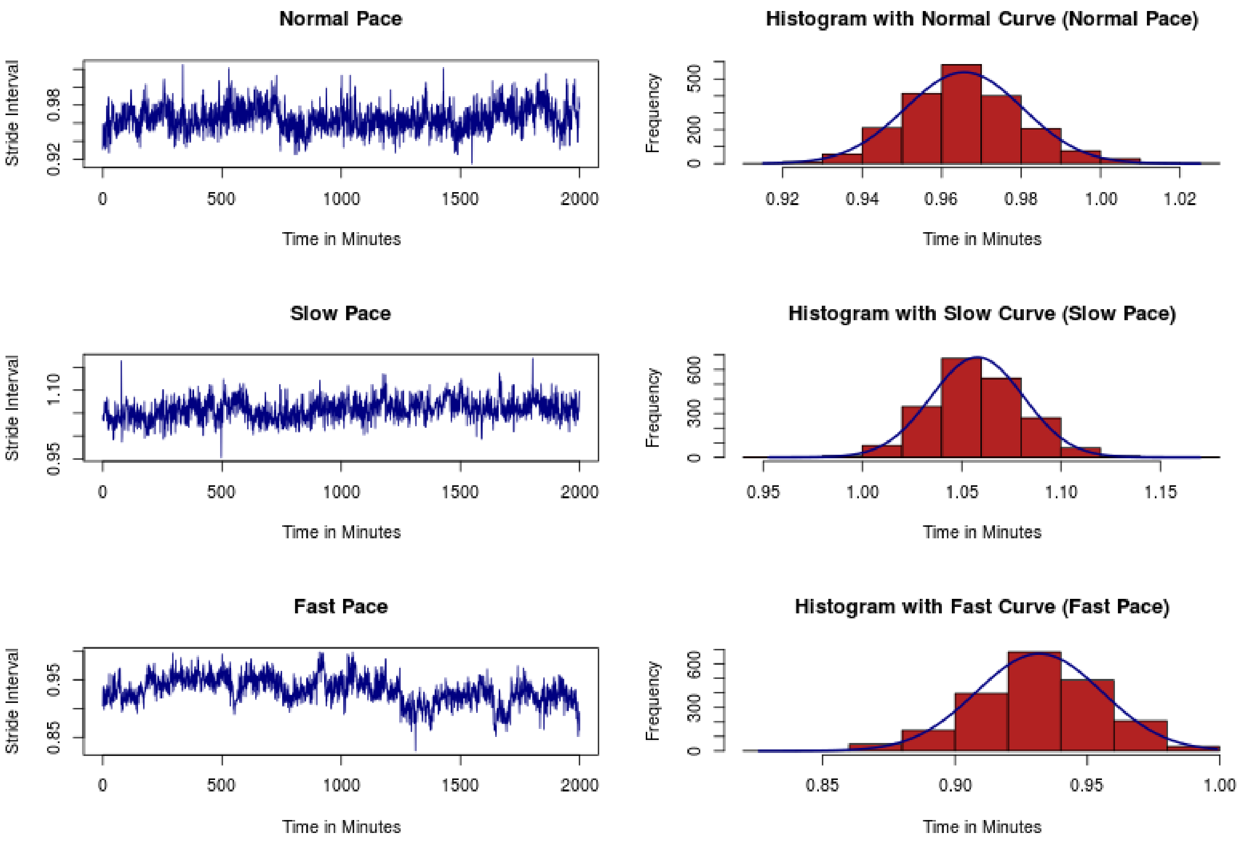

Figure 3.2: Distribution Plot for a User at Different Rates

fractal nature of human strides.

3.6 Classification Algorithms

In the following section, we discuss the classifiers that have been applied. Additionally, the results and observations are reported alongside.

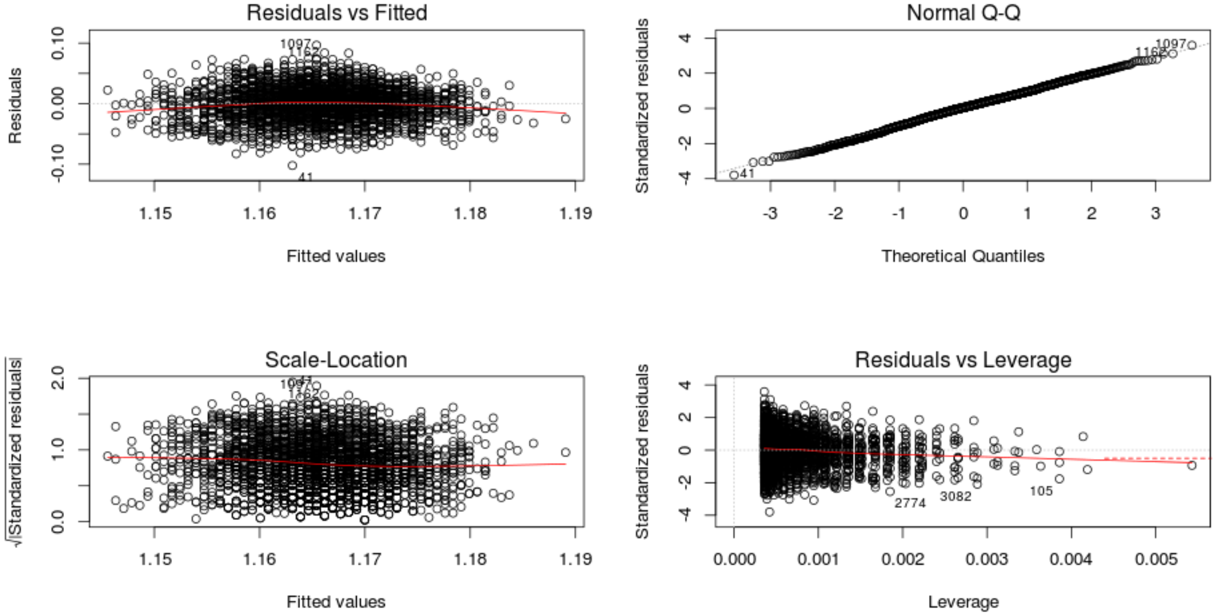

Figure 3.3: Homogeneity of Variance, (a) The expressed points showed a similar scatter for each condition, this is known as "homoscedasticity" (b) Plots the normality of the residuals, confirming the assumptions of ANOVA (c) Linearity between the growth of the residuals and the fitted values (d) Plot of appropriate factor level for optimum fit

Euclidean Distance Measure

Euclidean distance is perhaps the simplest measure that serves as a test of "similarity". Let $R = [r_1, r_2, r_3, ..., r_N]$ and $U = [u_1, u_2, u_3, ..., u_N]$, the Euclidean distance measure between the two vectors R and U is given by:

$$D(R, U) = \sqrt{\sum_{i=1}^{N} (r_i - u_i)^2} \tag{3.2}$$

For an "unknown" U the pairwise Euclidean distances $D(R, U)$, i = 1,2,..,n where n is the number of pattern vectors for different users in the database. The results observed are reported in Table 3.2. The reference template R is the set of collected gait data and U

Threshold	False Accept	False Reject
3	23.4%	0%
1.9	9.4%	0.4%
1.7	7%	1%
1.3	0.4%	7.2%

Table 3.2: The Euclidean distance is used as a similarity measure between the vectors

represents sampled data from the stored data reserve. The False Acceptance Rate (FAR) is the probability that the system incorrectly recognizes and authorizes a non-authorized person, this is caused when it incorrectly matches the obtained biometric input with the stored template. The False Rejection Rate (FRR) refers to the percentage of valid inputs which are incorrectly rejected. As seen for the observations noted, a threshold defined at 1.7 euclidean distance suggests to be the most optimal, with a FRR of 5 in 500, it has an accuracy of almost 93%. As the threshold limits are lowered, there is an observed drop in the values that satisfy the criterion of the filter (Figure 3.4). This can be attributed to the large loss of data in each of the profiles. As the overall acceptance rate drops, naturally the false acceptance rate exhibits a similar tendency, leading to a rise in the false rejection ratio. Thus, an optimal balance is needed which minimizes involved overhead.

Review of Gaussian Mixture Models (GMMs)

GMMs find high applicability in modeling the probability distribution of random events. By means of weighted L dimensional Gaussian functions, given that adequate training data is available, it can approximate any distribution. By definition, a GMM can be represented

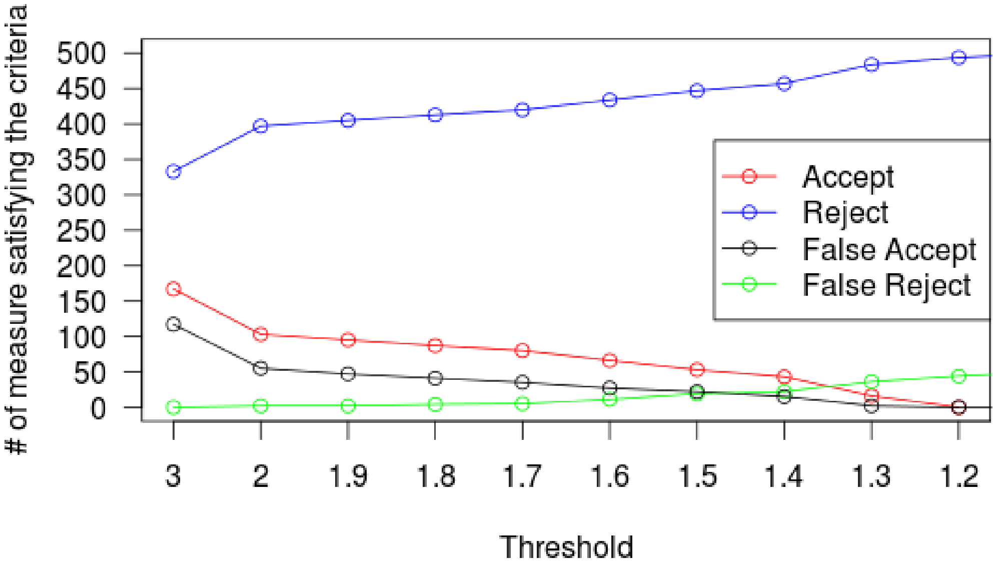

Figure 3.4: False Acceptance Rate vs False Rejection Rate

by the covariance matrix ζ_i, mixture weights ω_i and mean vector $\overline{\Psi}_i$, as represented below:

$$\Delta = \{\omega_i, \overline{\Psi}_i, \zeta_i\}, i = 1, ..., K. \tag{3.3}$$

Applying the model obtained from Δ, the likelihood $(\overline{z})$ belonging to the model Δ can be obtained by:

$$p(\overline{z}|\Delta) = \sum_{i=1}^{K} \omega_i b_i(\overline{z}), \tag{3.4}$$

where b_i is computed from a L-dimensional Gaussian probability density function (PDF) as expressed below:

$$b_i(\overline{z}) = \frac{1}{2\pi^{L/2}}|\zeta_i|^{-1/2} exp - \frac{1}{2}(\overline{z} - \overline{\Psi})^t \zeta_i^{-1}(\overline{z} - \overline{\Psi}). \tag{3.5}$$

To verify the likelihood that $\overline{z}$ does in-fact belong to the model Δ, natural logarithm is computed. This value is called as Log-Likelihood (LL) and is given by:

$$LL = log\{p(\overline{z}|\Delta)\} = log\sum_{i=1}^{K}\omega_i b_i(\overline{z}). \tag{3.6}$$

GMM Training and Verification

For generating an expected GMM, the user is required to enroll into the system. Each sample produces a single feature vector, thus n samples generate n feature vectors. The next stage would be to train the GMM, which is done by applying the expectation maximization (EM) algorithm. During verification, the user data is recaptured, associated feature vectors are extracted and finally compared with the user's model. Following that, equation 3.6 is applied to compute the log-likelihood that the given test vector ($\overline{z}$) obtained belongs to the model obtained before. The generated result is evaluated against the pre-determined user threshold before it can be accepted as a legitimate request. A key feature to be noted is that upon every successful authentication and validation of an individual; the GMM model and the threshold(s) for that user are modified with the new information and updated accordingly.

Calculating Model Threshold

For determining the threshold for a user, the LOOM (Leave One Out Method) is applied, which states that: for every N feature vector set that are extracted, $(N-1)$ vector sets are applied for training the model. Here the N^{th} vector (the last vector) obtained is being used to test the likelihood that it is a subset of that model (by applying equation 6). Given N

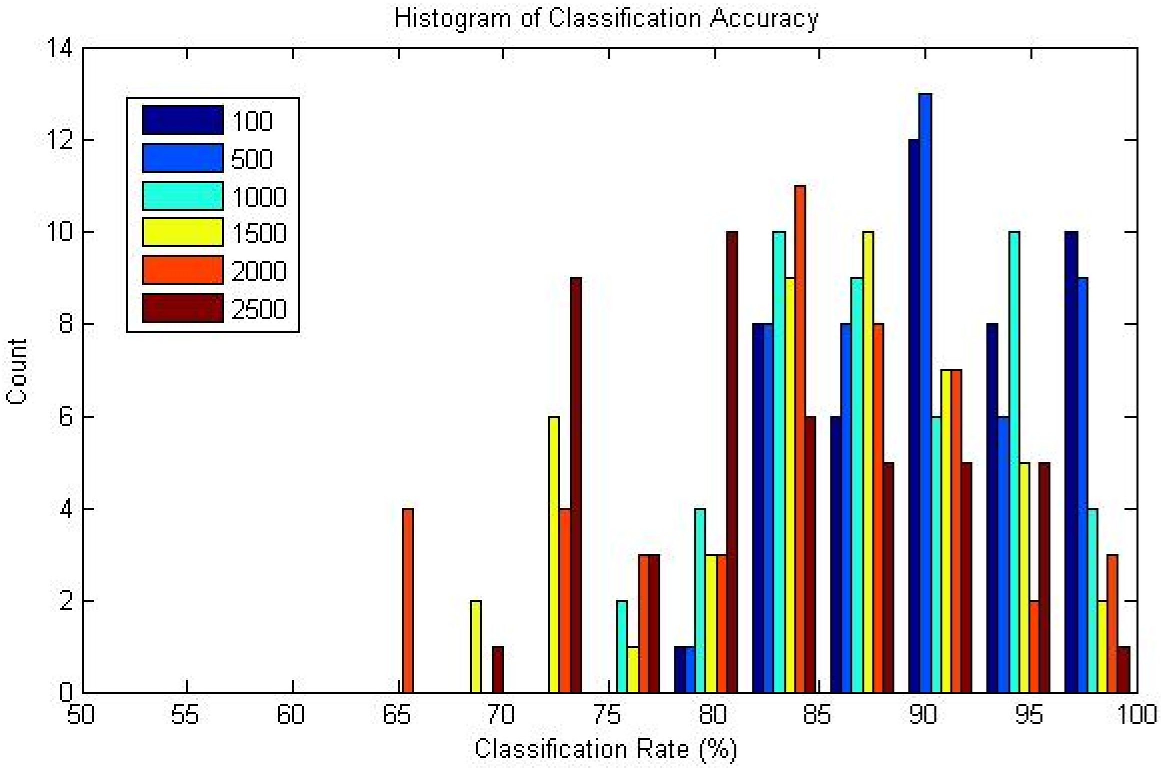

Figure 3.5: The Variance of Positive Classification Rate for Various Sample Size(s)

possible iterations, with every iteration a distinct vector is applied for testing the model. The final results generated may be represented by:

$$LL_i = log\{p(\overline{z}_j|\Delta)\}, j = 1, 2, ..., N. \tag{3.7}$$

Here, Δ is a GMM that has been trained with $(N-1)$ vector sets. This means that all the computations have been done while excluding the j^{th} vector, with the $\overline{z}_j$ being the test vector.

Results - Authentication using GMM

Given that authentication is the main goal behind applying GMM, the gait model should be such that it can produce a low FRR and FAR. Additionally, confusion matrix and classification performance rate are generated which are used to compute the acceptance/rejection parameters. The results for FRRs and FARs for 220 samples (obtained from Monte Carlo methods) are presented in Figure 3.5. A key feature to be noted is that the algorithm should fare well for computing FRR and FAR over time. This is due to its adaptivity in selecting an appropriate threshold that is the best defined for an individual user.

The results depicted show the variance of FRR and FAR over a varied sample space (from 100 samples to 2500 samples). These values span across a range from 0.1% to 8.0% using the aforementioned features. Our conclusion is that, smaller sample spaces exhibit better modelling prediction(s). The classification algorithm averaged a 87% positive classification rate, which is reasonably high (Figure 3.6). The trend that we observe is that FRR and FAR showed a consistent variance, thus illustrating the advantage of the adaptive modeling.

3.7 Biometric Key Generation

To our knowledge, biometric key generation algorithms are sparse and few, and none have been developed using gait as the primary physiological biometric. By applying multifactor authentication, our algorithm is targeted towards providing authentication between the coordinator and the host. For our purposes, we envision the coordinator as a FIFO

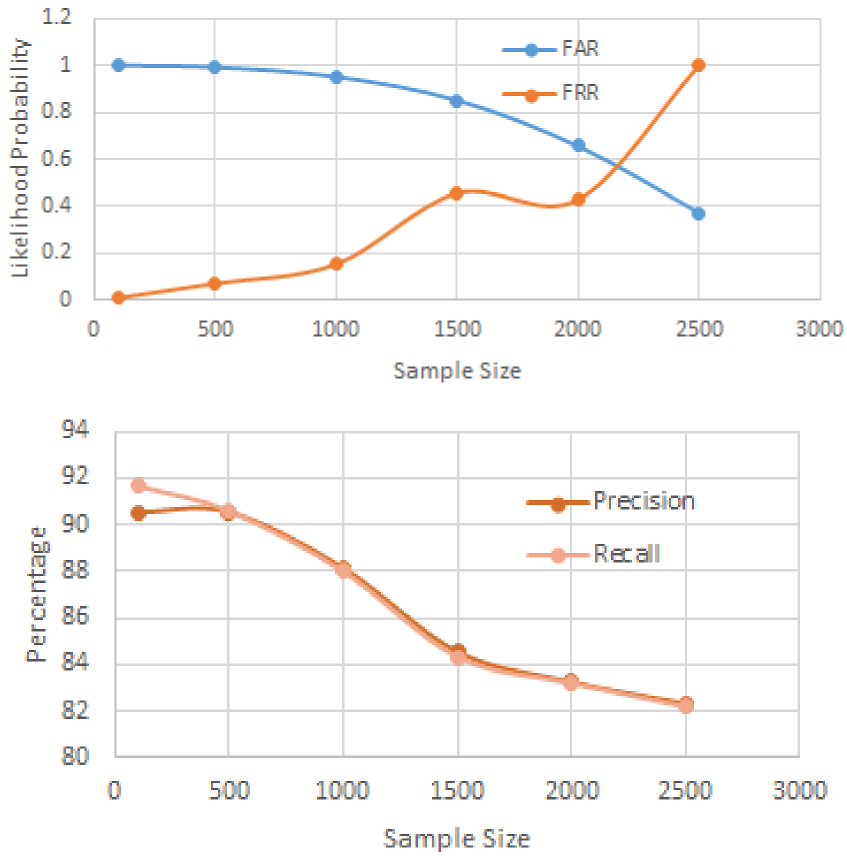

Figure 3.6: (a) Reflects the results of the GMM classification technique in terms of the False Acceptance Rate vs the False Reject Rate (b) Precision vs Recall as per the computations achieved from GMM classification

(First-In-First-Out) buffer, which is capable of storing the last (approximate) 50 samples that were generated. Communication properties being addressed by our scheme are: (1) Authentication, between the coordinator and the host, (2) Privacy and Confidentiality, (3) Non-repudiation, and (4) Protection against impersonation attacks.

Here, we present the algorithm and its associated components. The protocol consists of two phases, an enrollment period and a key-generation algorithm (Figure 3.7).

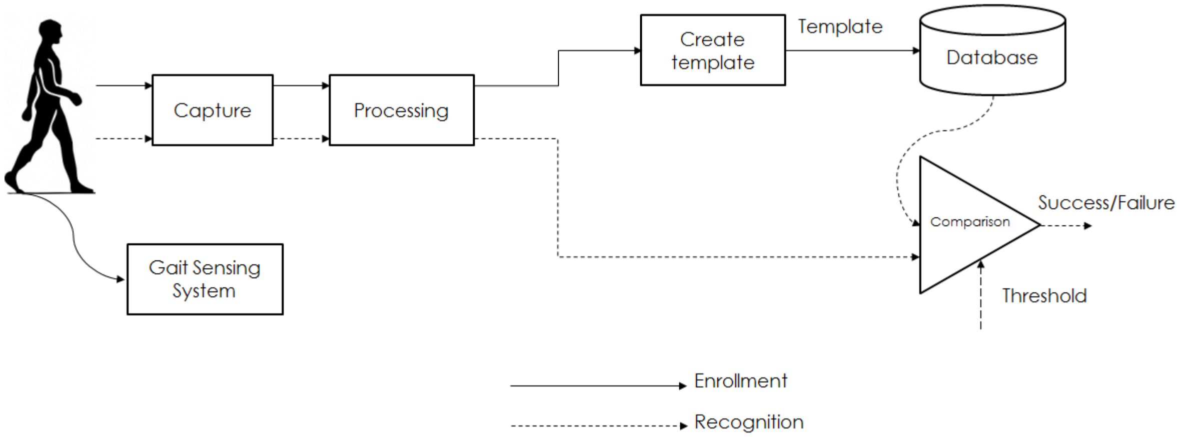

Figure 3.7: Outline of the System Information Flow; the Two Phases of the Proposed Scheme

- Enroll: The enrollment algorithm accepts as input the samples and generates a template against that user, which serves as the cryptographic key.
- Key-Generation: This algorithm accepts the samples as inputs, and generates the corresponding Message Authentication Code (MAC), which hides the generated key.

The algorithm has been modeled as a challenge-response system to a client-server paradigm with the client representing the coordinator, which provides the request to communicate and the server representing the host, which authenticates the user. The template generated is primarily server-side information which is stored for the purposes of regenerating the cryptographic key. Templates are usually created during the process of enrollment, and stored; and should be considered publicly available information.

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) has emerged as a promising alternative to RSA-based algorithms, it provides comparable security benefits using a smaller key size, while keeping it computationally inexpensive. Even though there have been several implementations and variations of ECC in WBAN, these are not the best alternatives. This is because the energy requirements in this scheme still remaind to be higher than those for symmetric systems [41]. Given such limitations, researchers have proposed applying ECC for infrequent and security-sensitive operations. In the proposed scheme, ECC has very restricted applications, during *Enrollment* and *Key-Generation* alone.

Multiple-Pass Depletion Method

Maximum Likelihood Estimation (MLE) is a technique which maximizes the known likelihood of a distribution. It is a standard approach in parameter estimation and for drawing inferences in statistics [42]. We apply the depletion method to estimate the capture efficiency, that is the captured sample and the outliers is applied to estimate the efficiency. We propose applying a multiple-pass depletion method for estimating population statistic, the estimation steps are:

$$T = \sum_{i=1}^{k} C_i, \tag{3.8}$$

$$X = \sum_{i=1}^{k} (k-i)C_i, \tag{3.9}$$

Here, i = pass number, k = number of passes, C_i = value of i^{th} sample, X = an intermediate statistic and, T = total time taken.The determination of the MLE of N is generated by:

$$\left[\frac{n+1}{n-T+1}\right]\prod_{i=1}^{k}\left[\frac{kn-X-T+1+(k-i)}{kn-X+2+(k-1)}\right]_i \tag{3.10}$$

The multiple-pass depletion method (MPDM) finds application is generating the template (or the cryptographic key) both at the coordinator and the host.

Tokenization

Communication begins when the coordinator raises a request to communicate with the host, which the host acknowledges. The coordinator then encrypts its own device ID using the aforementioned ECC algorithm, returning H_1. This is relayed to the server, which decrypts it to get back the device ID which raised the request. Now, both the server and the client have the same value of H_1, which we call as token and they serve as one-time parameters for exchange, akin to a session key. We reuse the tokens for determining the *Shift Index* denoted by t. The algorithm to achieve this is given as:

Algorithm 1 Generating the Shift Index

```
procedure Tokenization($Token$)
    $\sigma \leftarrow Token$
    $\tau \leftarrow zero$
    while $t/10 \neq 0$ do
        $\tau \leftarrow \tau + (\sigma \ \% \ 10)$
        $\sigma = \sigma / \ 10$
    $return\tau$
```

Modified Fisher-Yates Shuffle

The Fisher-Yates shuffle is an unbiased shuffling algorithm [43]. It works such that it swaps each item in the list with another item from the same list. With each iteration, the range of the swappable items shrinks. Initially, the algorithm starts at an index zero, and randomly chooses an item from [0,N]. This selection locks the 0th element in the shuffled list. During the next iteration, a random item from 1 to N is selected. This continues for the total length of the list. In the modified Fisher-Yates algorithm, instead of randomly choosing an index location during every iteration, it applies the previously computed *Shuffle Index* as the index whose variable at that location has to be interchanged. With every iteration, the substring on which the shuffle algorithm is applied is different, thus the *Shuffle Index* references a different variable everytime. The algorithm is illustrated as Algorithm 2. By shuffling the generated physiological values, privacy of the user information is ensured. As such, even if the user information is overheard during communication, the attacker will be unable to decipher the original value unless he/she has knowledge of the token value, and the tokenization and the shuffling algorithms.

Algorithm 2 Modified Fisher-Yates Shuffle

```
procedure ModFY($str1, sindex$)
    $i \leftarrow 1$
    for $i <$ len(str1) do
        $temp \leftarrow str[sindex]$
        $str1[sindex] = str1[i]$
        $str1[i] = temp$
        $i \leftarrow i + 1$
    return $str1$
```

Levenshtein Distance

Most standard biometric verification protocols deploy Hamming distance as the metric for determining the similarity between two strings (or sample values). However, the Levenshtein distance measure is more sophisticated as it can be defined for strings of arbitrary lengths. It is a metric for computing the difference between two input sequences (denoted as *Levenshtein(* δ *,* ϵ *)* and is defined as the minimum number of operations required to transform δ into ϵ, which is solved using dynamic programming. It finds wide application in pairwise string alignments (such as DNA sequencing)

Enrollment Algorithm

The enrollment algorithm is applied when an individual is enrolled into the system, which is once per user. The user wears the coordinator (client) on his/her body which attempts to communicate with the host recognition system (server). The proposed algorithm serves to relay the device ID to the host, capture the biometric sample(s) from the user, update the coordinator buffer and relay the samples to the host. At the host, the sample is stored and the corresponding template is generated and stored. Storage has been designed such that against each user, (a) a device ID, (b) a template, and (c) a biometric sample (size N) are stored for recognition purposes.

Algorithm 3 Coordinator (Client)

```
procedure ClientEnroll
    $Req\ to\ Communicate(ClientTimestamp) \rightarrow Server$
    $\tau \leftarrow tdiff\ from\ Server$
    $H_1 \leftarrow ECC(\ ID \bigoplus \tau)$
    $H_1 \rightarrow Server$
    $Capture\ Sample(\eta_k) \rightarrow Server$
```

Algorithm 4 Host (Server)

```
procedure ServerEnroll
    while True do
        $Receive\ Request\ and\ ClientTimestamp$
        $\tau \leftarrow \mid ServerTimestamp - ClientTimestamp \mid$
        $Send\ an\ acknowledgement(\tau) \rightarrow Client$
        $H_1 \leftarrow Receive\ from\ Client$
        $H_1^{'} \leftarrow D_{ECC}(H)_1$
        $ID \leftarrow H_1^{'} \bigoplus \tau$
        $Receive\ \eta_k$
        $\Theta \leftarrow MPDM(\eta_k)$
```

Key Generation Algorithm

Once sample has been collected, a template is generated and stored at the server side, and the user is now able to raise a recognition request to the host when required.To do so, the Key-Generation algorithm is applied to authenticate the user against the device, before communication can be enabled. Having acquired the device id, the biometric template is matched against the generated biometric parameter derived from the aforementioned likelihood estimation techniques. If the sample is within bounds of the determined threshold, post processing is done and the user is authenticated. Valid user authentication and generation of a Message Authentication Code (MAC) is the second phase of the proposed authentication protocol.

Algorithm 5 Coordinator (Client)

```
procedure ClientKeyGen
    $Req\ to\ Communicate(ClientTimestamp) \rightarrow Server$
    $\tau \leftarrow tdiff\ from\ Server$
    $H_1 \leftarrow ECC(\ ID\ \bigoplus \tau\ )$
    $H_1 \rightarrow Forward\ to\ Server$
    $t \leftarrow Reduce(H)_1$
    $\eta_{BRF} \leftarrow MPDM(\eta)$
    $\eta'_{BRF} \leftarrow Shuffle(\eta_{BRF})^t$
    $MAC \leftarrow \eta'_{BRF} \bigoplus ID$
    $MAC \rightarrow Server$
    Decision: Yes/No
```

Algorithm 6 Host (Server)

```
procedure ServerKeyGen
    while True do
        $Receive\ Request\ and\ ClientTimestamp$
        $\tau \leftarrow \mid ServerTimestamp - ClientTimestamp \mid$
        $Send\ an\ acknowledgement(\tau) \rightarrow Client$
        $H_1 \leftarrow Receive\ from\ Client$
        $H'_1 \leftarrow D_{ECC}(H)_1$
        $ID \leftarrow H'_1 \bigoplus \tau$
        $t \leftarrow Reduce(H)_1$
        $Load\ \Theta_{ID}$
        $\Theta'_{ID} \leftarrow Shuffle(\Theta_{ID})^t$
        $Receive\ from\ Client \leftarrow MAC$
        $\eta'_{BRF} \leftarrow MAC \bigoplus ID$
        $Levenshtein\ Distance(\ \Theta'_{ID}\ ,\ \eta'_{BRF})$
    Decision: Yes/No
```

3.8 Results

Overall Performance

The proposed algorithm has been tested using the aforementioned dataset, which consists of 50 samples from 10 people. Each person is assigned a random device ID, and a biometric template for each was generated (satisfying the constraints as stated above). For example, say a person Alice is to be enrolled into the system, she will have: 5 sample datasets recorded against her, a device ID associated with her identity and a template stored at the server side. Upon initiating a request to communicate with the host, a random dataset from the 5 is selected and the proposed recognition scheme is applied. To determine whether Alice is who she claims to be, her device ID will be used to determine the template at the server side. Similarly, current physiological information generated from Alice's coordinator will be used to determine the identity of Alice as being valid or not, as claimed. If Alice is authenticated, communication will resume and the computed MAC (message authentication code) will be used for all future communication.

Having accounted for positive identification of legitimate users, we analyzed the case where Bob claimed to be Alice by wearing Alice's coordinator. In this scenario, information we have are: (a) Alice's template associated with her device ID, (b) Alice's device ID being used by Bob, and (c) Bob's physiological information being stored in the coordinator buffer. When Bob attempts to communicate with the host, Alice's device ID will be relayed to the host. The host will then pull up Alice's template from storage and using the proposed algorithm(s)

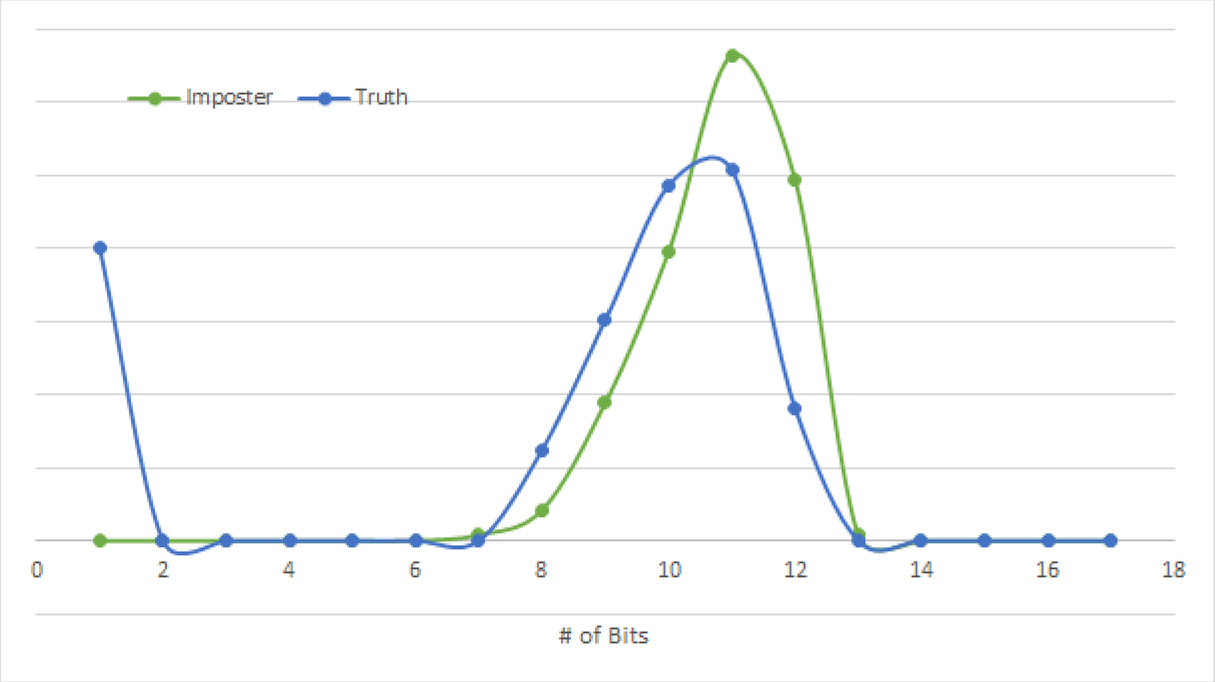

Figure 3.8: Histogram of Genuine and Impostor results

attempt to verify Bob's claimed identity by comparing it against Bob's most recent gait information. To test the performance of the proposed scheme, both the genuine and the impostor user identity scenarios (Figure 3.8) are executed for one million iterations before generalized results could be presented. In general, FAR comes out to be inversely proportional to FRR. As such, a reduction in the value of FAR will cause an increase in FRR, and vice-versa. For a designing an optimum recognition system, it is advised to have a balanced results between FRR and FAR. This is where the threshold value finds application, it is used to investigate the best possible combinational value of FAR and FRR. The consequences of using different threshold values will bring about a change in the performance of the FRR and FAR metrics. In our design, a low threshold value reflects a strict authentication process and

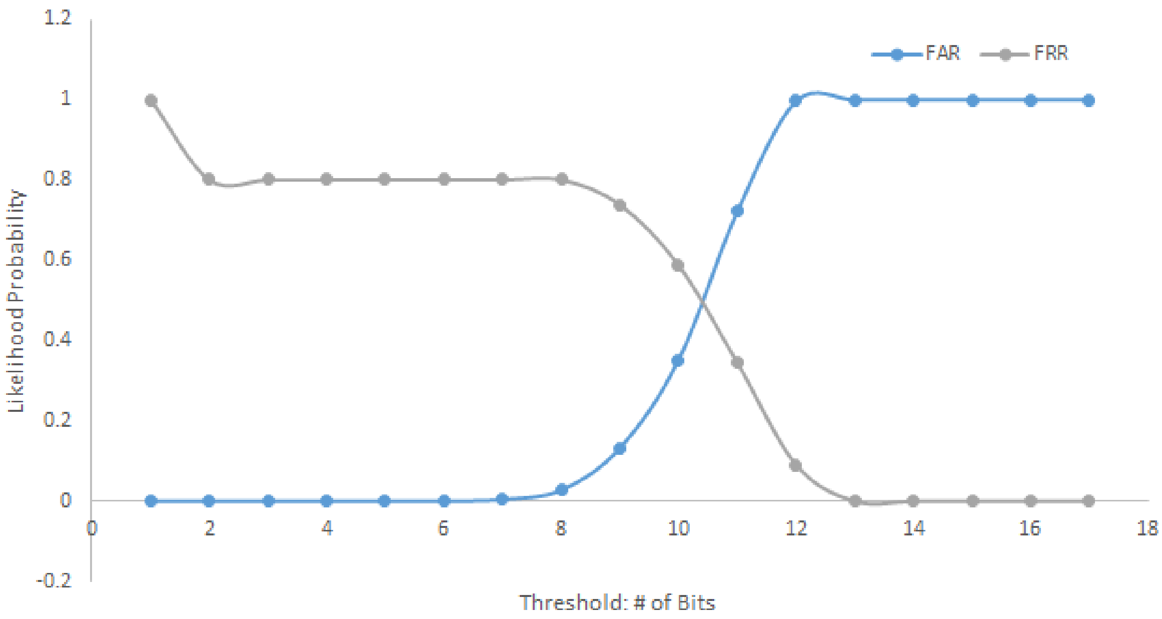

Figure 3.9: FAR vs FRR

will produce a low FAR but a high FRR (Figure 3.9). However, an increase in the threshold value will lead to a drop in the value of FRR and a rise in FAR. For our experiment, the optimal threshold value obtained is defined when the Levenshtein Distance is 9. Here, the positive identification success rate is at 80% and it rejects 86% of impostors. When the threshold is defined at 0 bits, the system is capable of positively recognizing around 20% of the users as valid while rejecting all impostors who try to gain access. However, given the nature of biometric data, this threshold is not reasonable and thus, it is not acceptable. If the threshold is defined at a distance of 11 bits, the system is capable of recognizing 91% genuine users while rejecting 28% of impostors.

3.9 Conclusion and Future Work

We studied the gait characteristics as a user authentication biometric and established its uniqueness with respect to a user. We applied various classification techniques and proposed a new timing metric which suppresses outliers, normalizes feature variations and decouples correlated data. Given the nature of *stride interval*, it can be applied across the board for various applications. In future, we plan to investigate use of this metric with a more varied dataset; considering different stances of human movement and the application of hybridized biometrics for authentication purposes.

The purpose our proposed scheme is to rightly identify the user and the device associated with the user before communication can be established. From our results, we can conclude that while gait is a reasonable metric, the inherent nature of gait dictates that is it is better suited as a passive biometric. While we used the new metric to test the proposed scheme, both the metric and the scheme are independently applicable. We aim to address this in the future, and hope to propose novel applications and solutions.

Chapter 4

Applying Merkle Trees to WBAN

4.1 Introduction

A Wireless Body Area Network (WBAN) is a network consisting of resource constrained wearable devices which provide constant and remote monitoring of human physiological parameters in real-time. One of the end goals of this architecture is to relay this information to a medical server or professional for off-site processing and analysis. An array of wireless sensors available today have facilitated the design of more sophisticated health care monitoring systems, with such systems providing greater accessibility to the users. However, at the opposite end of the spectrum, such convenience makes the user's privacy susceptible to compromise.

Chapter is based on *"A Hybrid Key Management Scheme for Healthcare Sensor Networks,"* published in IEEE International Conference on Communications (ICC), 2016 [44].

The security and privacy of medical data has been an indispensable component of WBAN system design, with authentication and access control being one of the key requirements. Given, the nature of the data and its multi-platform interaction; it is more vulnerable to eavesdropping attacks as information is relayed across open wireless channels. One of the biggest problems faced by WBAN devices is node compromise as these devices are easy to capture and manipulate. A node is said to be compromised if its' secret key(s) are leaked. If the information stored on such devices is not encrypted, it could lead to the eventual collapse of the entire WBAN. The rapidly changing network dynamics and topology, as a result of human motions, may result in nodes dying out prematurely. This could potentially affect the network performance, thus proving to be a possible security issue. Setting up of secret keys between nodes is a known problem in wireless sensor networks (WSN) and WBAN, and is formally known as the *key agreement* problem.

Symmetric cryptography, due to its greater performance efficiency, is considered an appropriate solution towards designing security solutions. Pre-distribution of keys among sensors is a long standing practice in WSN, however such schemes suffer from poor connectivity, high memory demands and low resilience. Biometric solutions have also been proposed as a possible alternative, however they are far from being a "plug and play" solution. Public Key Cryptography (PKC) is capable of addressing those issues as identified before. PKC has found large applications in securing the Internet, mostly for bootstrapping communication. While PKC has been criticized for their added complexity and computation requirements, more recently, researchers have shown the viability of using Elliptic Curve Cryptography

(ECC) as a feasible solution for both WSN and WBAN. Given its limited energy requirement, small key size and small signatures, ECC has been applied in various flavors to facilitate secure communication in WBAN. Researchers have verified that a 160-bit ECC key provides comparable strength to a 1024-bit RSA key [45]. Applying Moore's Law, one can argue that PKC will one day emerge as an optimal solution for WSNs. However, even as the performance of PKCs improve, symmetric cryptography will always outperform the former. Given its known limitations, PKCs should be adopted with caution as they still prove to be expensive operations. Thus, it is recommended that the use of PKCs be more selective and more restrained, with the goal of maximizing the overall network lifetime. Additionally, researchers have proposed that the use of ECC be limited for infrequent and security-sensitive operations alone [46]. With this research, our focus is on the optimization of PKC algorithms, rendering them more efficient for the sensor nodes.

The main contributions of our research are:

1. We propose a novel architecture that ties together traditional symmetric key distribution techniques with asymmetric cryptographic methodologies,

2. We propose a new optimized technique for public key authentication operations, thereby reducing the network overhead across multiple sub-processes, and

3. We verify the identity of the public keys using minimum cost, and also addresses the problem of identifying compromised nodes

4.2 Related Work

Providing security solutions for healthcare applications is an active area of research, with wearable health solutions garnering high interest amongst researchers. Given the joint nature of interest from both government and industrial laboratories, a wide range of solutions have been proposed. *HealthGear* is a wearable real-time monitoring system consisting of wearable sensors [47]. This system communicates over Bluetooth and provides on demand analysis of physiological signals. With *Ubimon*, researchers address the issues associated with wearable and implanted sensors for distributed mobile monitoring [48]. *CodeBlue* has been proposed as a disaster response system, seeking to integrate various sensor devices across a wide array of sensor platforms [49]. The proposed systems were designed with the goal of providing cost effective and power efficient solutions. However, the security related issues in WBANs are similar in nature to those of WSNs. But the solutions for the latter do not necessarily apply for the former. Privacy and security issues in such systems are one of the prime concerns raised by researchers, and have been appropriately addressed in [50]–[53].

Symmetric key cryptography has seen several solutions being proposed for traditional WSNs. Eschenauer and Gligor [54] (referred to as the basic scheme) designed a probabilistic key-distribution technique for WSNs, with the aim of providing initial trust amongst sensor nodes. This idea was further built upon by Chan et al. [55], who proposed the q-composite key distribution scheme. As per this scheme, two nodes may only establish a mutual key only when they share at least q keys. Researchers have also proposed more context aware schemes,

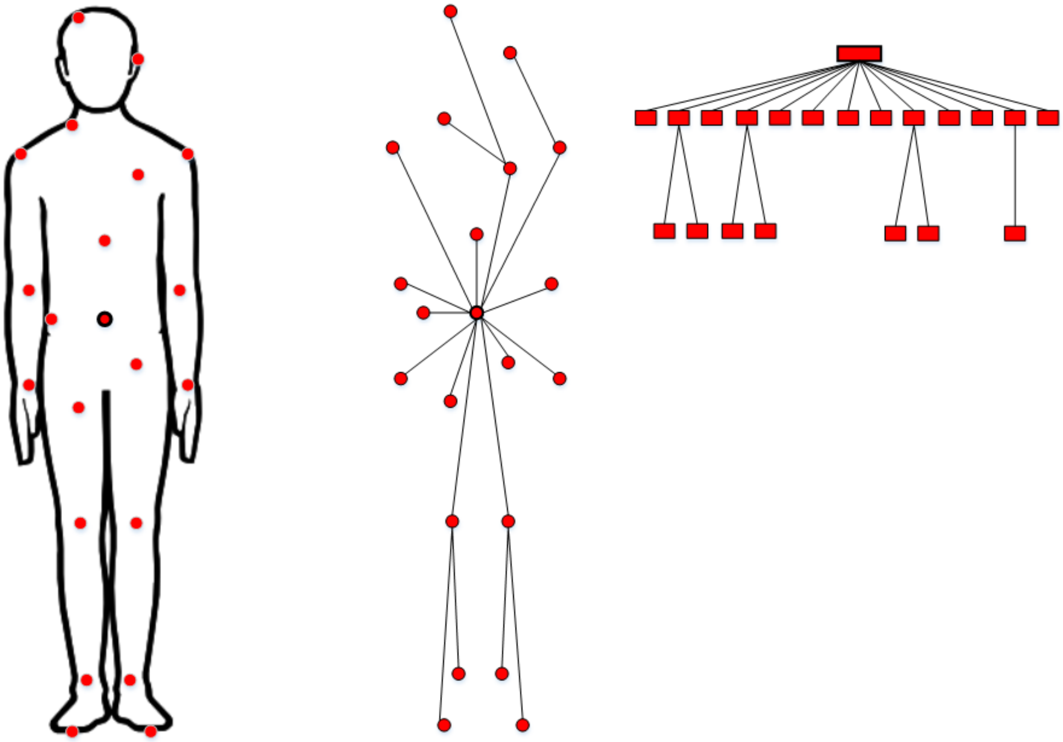

Figure 4.1: Building a Sensor Topology for WBAN: A snapshot of an instance of a network topology and the resultant tree formed from the topology (based on hops from the coordinator). The coordinator is located at the center of the frame and forms the root of the resultant tree

aimed at providing solutions for topology aware network schemes [56]. The latter proved to be more memory efficient and provided better connectivity amongst the sensor nodes.

4.3 Proposed Authentication Scheme

Traditionally, public key authentication exists to legitimize the binding between the public key of a node and its claimed identity. While conventional applications require the use of a Certificate Authority (CA) to verify this binding, sensor nodes work under the assumption that the nodes have already established a relationship before deployment. As such, they exist in a benign environment wherein they may exchange information in plaintext, with the aim of establishing a trust relationship between/amongst themselves.

Preliminaries

In the proposed system model, users have sensor enabled devices on their form (on or inside their body). These devices communicate with a personal server, Γ. As per the IEEE 802.15.6 standards defined for communication in WBAN, the network topology has been proposed as a 2-hop star network, with Γ serving as the local hub in Figure 4.1. In addition to the aforementioned functionalities, Γ also serves as the gateway access point between the WBAN and the Internet. Thus, a typical WBAN coordinator is assumed to possess functionalities or processing power akin to a modern smartphone. Hence, it is inferred that Γ is capable of storing and performing computations of higher orders as compared to the other sensor nodes.

A Trusting Scheme

An unsophisticated solution where public key authentication is achieved (without applying certificates) is where each sensor node carries public keys to all other sensor nodes in the network. The potential downside of this scheme is its excessive storage requirements. If the size of the public keys is large, the sensor node might not possess sufficient memory to store all the keys. This can be improved upon by having each sensor node carry the hashed value of the same keys. Typically, if Q bits are required to store a key, then its identifier will require $log_2(Q)$ bits. Consequently, when a sensor node receives the public key from another sensor node, it computes its one-way hash value and determines if the generated value matches the one stored in its memory. However, this scheme is far from being perfect and still poses memory-associated problems. The storage overhead in both scenarios prove to be impractical for use as illustrated by our research.

Merkle Hash Tree

Merkle trees are a class of hash trees that provide multiple cryptographic applications, including access control and authentication. These are trees based on a one-way hash function, where leaf nodes may be verified by means of its authentication path information (API). The computation costs are kept at a minimum as only the hash functions have to be computed [57].

A Merkle tree is a complete binary tree, consisting of a hash function $\hat{h}$ (like MD5, SHA-2) and its corresponding assignment Φ, which maps the hashed value of the concatenation of the Φ values of its children. By applying a recursive one-way hash function, Merkle trees offer an efficient storage and retrieval technique. Thus, if we assume that Nl and Nr denote the left and right roots of a node, the value Φ is computed by

$$\Phi(N) = \hat{h}(\Phi(Nl)||\Phi(Nr))$$

Phases of Key Management

Taking inspiration from [54], key distribution scheme can comprise of two primary phases namely: key-distribution and shared-key discovery. Similar to [54], a large pool of P keys and their corresponding key identifiers are generated. This is done by means of one-way hash function (denoted by $\hat{h}()$) for each key. The main differentiator between our scheme and the basic scheme is the usage of asymmetric keys. As such, key generation involves a private key, a public key and its resultant public key identifier. Once P has been generated, a set of random public keys and their corresponding identifiers will be loaded onto the sensor nodes.

The topology of the network is determined during the shared-key discovery phase. Here, a link may exist between two nodes if they share a common key. In the adopted trust model (Figure 4.2), Γ acts as the key distribution server, thus is a trusted entity in the network hierarchy. Γ may be a smartphone or a personal digital assistant (PDA) depending upon the scenario being taken into consideration. We describe our deployment environment as a heterogeneous network consisting of a wide array of sensor enabled "smart" devices which may be manufactured by the same or different vendors, all of which communicate with a common access node (Γ). As part of the trust model, we assume that Γ is preloaded (hard-wired) with a master key pair ($M_{private}$ and M_{public}). In addition to this, Γ also stores a set of key pairs (public and private), which is referred to as the key pool P. When a device enrolls itself with Γ, it is assigned an identifying node ID (N_i), where $i = 0, 1, ..., m$ and a set of n random public keys from P. This is known as the key ring and is denoted by K_i, such that

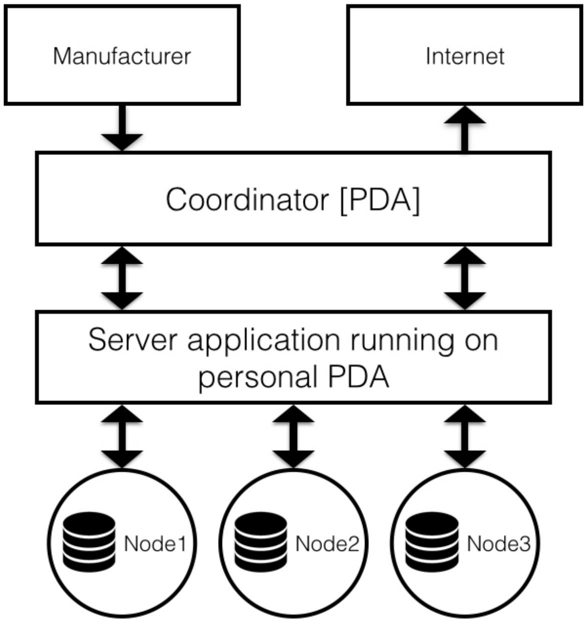

Figure 4.2: The Trust Model

$K_i \leq P$ where $i = 0, 1, ...m$. Here, m denotes the total number of devices connected to Γ, traditionally known as the network size. In addition to the key ring, each node also acquires M_{public} and its hash (hM), and the hashed values for each key from K_i. Thus, each node stores: $[N_i, K_i, \hat{h}(K_i), M_{public}, \hat{h}(M_{public})]$.

As per the 802.15.6 standards, it is known that a node could exist in one of two states: relay and sensing. In the sensing state, it receives physiological information as a direct source, and forwards the same to Γ. In the relay mode, the device receives physiological information from another sensory device with the intention of forwarding the same to Γ. Once the keys have been randomly distributed to the sensor devices by Γ, they are placed at their respective

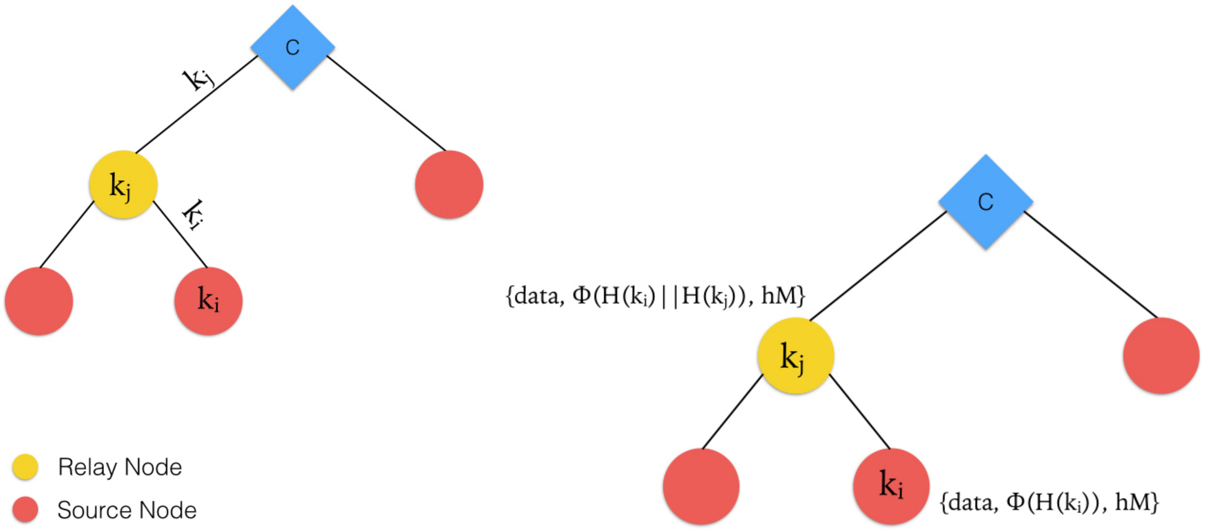
C
k_j
k_j
k_i
k_i
Relay Node
Source Node
C
$\{data, \Phi(H(k_i)||H(k_j)), hM\}$
k_j
k_i
$\{data, \Phi(H(k_i)), hM\}$

Figure 4.3: Establishing Communication in WBAN (L-R): (a) represents how links are established between nodes, (b) is a representation of the payload exchanged between nodes, originating at the sensing node and terminating at the coordinator, via the relay node

sensing points. Using the routing layer as the foundation, the shared-key discovery process is initiated. This could be achieved in several ways. A naive approach would be to have two nodes broadcast their key identifiers as plain text. This is advantageous as the attacker does not have access to information that he/she is not already privy to. For example, two nodes s_i and s_j wish to communicate with each other. Either one of the nodes may communicate its list of identifiers to the other, say s_i forwards its identifier list to s_j. s_j determines if there is a matching value in the identifier list, and it uses the corresponding key to encrypt the information. It is worthwhile to note that it's possible for two nodes to share more than one common key between them, as the keys have been randomly selected and allocated to each node.

Once s_j encrypts the information sensed by it using the mutually shared key k_i, it forwards the same to node s_i along with the hM stored by it and the value of Φ as computed (Figure 4.3). Thus, it relays

$$s_j \xrightarrow{k_i} s_i = [data, \Phi(\hat{h}(k_i)), hM]$$

The node s_i identifies that the information received is from a trusted source by verifying hM as received as part of the payload. It is assumed that a node will hold a valid value for hM only if its been trusted by Γ. In this specific case s_i acts as a relay node, thus it will forward the received encrypted data packet to the intended destination node (coordinator). s_i establishes k_j as the mutual key between itself and the coordinator, and forwards the data packet to the coordinator. As an added security solution, s_i may also encrypt the data packet with the key k_j. Thus, s_i communicates to the coordinator (Γ)

$$s_i \xrightarrow{k_j} \Gamma = [data, \Phi(\hat{h}(k_i)||\hat{h}(k_j)), hM]$$

The relay node will perform a one-way hash computation on the result obtained by concatenating the identifiers of the keys k_i and k_j. Once the coordinator receives the data packet from s_i, it verifies the legitimacy of hM. Once, s_i has been established as a trusted source, Γ extracts the Merkle hash value and verifies if the computed hash value is legitimate by means of a lookup table.

If the value represented by Φ is determined to be genuine, the coordinator will decrypt the data using the private key for k_j. In case a double encryption was adopted, the coordinator will decrypt the information using the private keys against k_i and k_j respectively. It is important to note than in case of the latter scheme, it is extremely critical to protect the order of encryption. In case of a sensing node is 1 hop away from the coordinator, the scheme works in a manner similar to communication between nodes s_j and s_i, with the processing at the coordinator being similar as before, without the overhead of having to traverse the lookup table to determine which keys were used for encryption (and in which order, if needed). Thus, in this manner, the coordinator successfully receives and decrypts the information as originated in node s_j.

If the value of Φ is not one that is available in the lookup table, Γ will infer that one of the two nodes from which the information was received, has been compromised. As such, it will raise a challenge to the network, as detailed in the next section.

Building the Lookup Table

The lookup table is used to determine the key(s) that are used to perform encryption, the order in which the keys are used, to identify whether a discrepancy has occurred and to render support for determining node compromise. All this while maintaining a lookup complexity of $O(1)$. Table 4.1 does a $(key, value)$ mapping, where:

Key	**Function**	**Value**
$\hat{h}(k_i)$	Identifier	Corresponding Private Key
Φ	Merkle Tree	Key identifiers (order preserved)
χ	HeartBeat Package	XOR of all identifiers

Table 4.1: Understanding the lookup table nomenclature

HeartBeat Package

The HeartBeat Package (*HBP*) is designed to perform network re-traceability and diagnostics, with the goal of combating Denial-of-Service (DoS) attacks. Similar to a beacon signal, the coordinator broadcasts a challenge to all the nodes defined in the WBAN. As a response to the received challenge, each node returns:

$$\begin{gathered} HBP_i = [N_i, (\hat{h}(k_x) \oplus \hat{h}(k_{x+1}) \oplus ... \oplus \hat{h}(k_n)), hM], \\ where\ k_{x,...,n} \in K_i\ and\ i = \{0, ..., m\}. \end{gathered} \tag{4.1}$$

Network diagnostics is important as it helps identify unreachable nodes, which in turn implies that a potential DoS attack has occurred as a direct result of possible node capture and/or node reset or reformatting, rendering the node unavailable. The HeartBeat Package works in a manner as outlined below:

- The coordinator computes and stores the result of all of the possible values returned by χ, where $\chi = (\hat{h}(k_x) \oplus \hat{h}(k_{x+1}) \oplus ... \oplus \hat{h}(k_n))$,
- χ computes the logical XOR on all the public key identifiers from a key ring present in a node and stores the same as a lookup table, to improve response time,
- The coordinator broadcasts a challenge to the entire network,
- Each node in the network replies back with the packet as illustrated in equation (4.1),
- The coordinator extracts the Node ID (N_i) and $hM$to determine if all the nodes have been accounted for; hM verifies that the node is one that is trusted by the coordinator,

- The coordinator queries the value returned by the function χ and verifies if it is valid or not, and
- If the value returned is legitimate, the node is declared untampered. However, in the case where the value does not match any of the ones present in the coordinator's memory, we can declare that the node has been compromised and requires physical intervention

A typical WBAN may be programmed to invoke *HBP* at regular intervals of time or during phases when the overall response time of the system seems to be below a certain pre-determined threshold value, suggesting a possible network congestion. The *HBP* serves to account for the presence and availability of all the sensor nodes in the network, and to identify compromised sensor nodes, if any.

Key Revocation

Once a compromised sensor node has been identified, it is important to revoke the key ring (K_x) of that node. The coordinator broadcasts a list of k key identifiers to all the nodes in the network, as a single revocation message. The revocation message is signed by $M_{private}$ before it is broadcasted to all sensor nodes. The receiving nodes verify the authenticity of the signed list of identifiers, pinpoint on the identified key identifiers, and revoke communication privileges for the corresponding keys (if any). It is worth noting, that once encryption-decryption properties are revoked for certain keys, the network topology and connectivity is altered as well. While the overall effect on connectivity of the topology is small, it causes the desired affect of isolating the compromised node.

Deployment Knowledge Modelling

WBAN are unique in that they form a hybrid network topology consisting of static and dynamic components. The *deployment point* of a sensor node is the point at which the node is deployed initially, not where it resides finally. Typically, a WBAN sensor device has specific deployment points, which determines approximately what the communication distance between itself and the coordinator is likely to be. As such, it can be estimated whether a node will be 1-hop or 2-hops away from the coordinator, as a general rule. In this work, as an additional incentive, we model the distribution of the keys amongst the nodes as a ruled based scheme. The rules have been defined as follows:

- *Random Key Pre-Distribution*: The size of K_i is assummed to be the same at all nodes
- *1 Hop-Heavy Random Key Pre-Distribution*: The size of K_i at the nodes 1 hop away from the coordinator is more than the nodes which are 2 hops away,
- *2 Hop-Heavy Random Key Pre-Distribution*: The size of K_i at the nodes 2 hops away from the coordinator is more than the nodes which are 1 hop away, and
- *Priority driven Random Key Pre-Distribution*: Certain "critical" nodes have been determined to possess a higher priority, therefore requiring higher connectivity. Thus,

the size of K_i in these nodes are larger to enable improved fault tolerance.

Here, K_i refers to the key ring at node i.

4.4 System Analysis

Considering the resource-constrained nature of WBAN devices, it is important to investigate the impact of the proposed authentication protocol.

Communication Overhead

Given the inherent nature of the network topology as being one where communication is restricted to a 2-hop network, communication overhead is at a minimum. This is because the height of the Merkle Tree directly influences the information exchange that occurs through the rest of the network. The maximum height as per our scheme is limited to 2. Assuming a network size of m, with n hash values being stored by each node. the average communication overhead is approximately $(log\frac{m}{n})$.

Memory Overhead

When proposing a new scheme for establishing security, a compromise has to be made between storage and communication. Taking into consideration the limited storage available on the sensor nodes, and the relatively better storage capacity of the coordinator, our scheme is designed to cater to such network constraints. Each sensor in the network is required to

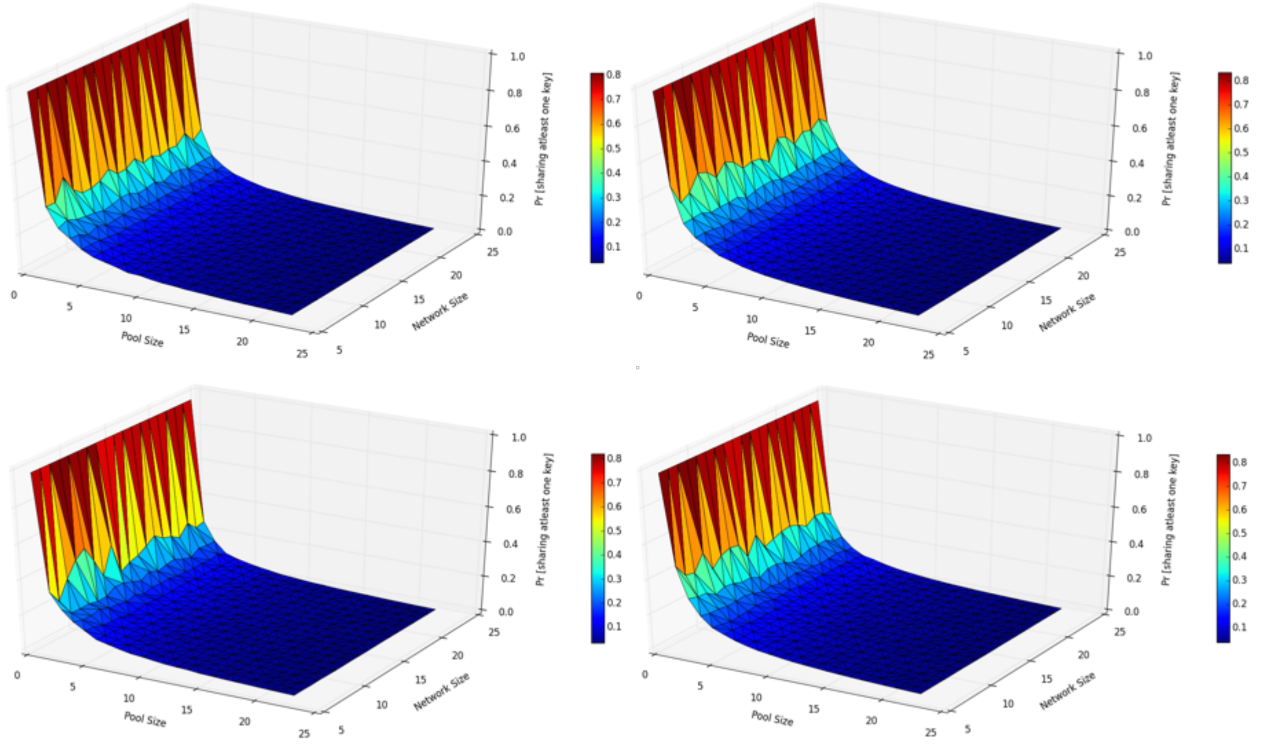

Figure 4.4: (a) Random Key Pre-Distribution(b) 1 Hop-Heavy Random Key Pre-Distribution, (c) 2 Hop-Heavy Random Key Pre-Distribution, (d) Priority driven Random Key Pre-Distribution. The plots represent how the probability of two nodes being connected varies with respect to varying network size and pool size. The axis being represented are: (i) x-axis: Pool Size (ii) y-axis: Network Size (iii) z-axis: Pr[probability of sharing at least one key]

Table 4.2: Character Reference Guide

Character	**Denotes (size of)**
α	Node ID
σ	Digital Signature
ζ	Public | Private Key
ξ	Public | Private Key Identifier

store: *[#NodeID, Key Ring, Key Ring Identifier, Master Public Key + Hash.* Thus, each node stores

$$S = \alpha + (|K_x| + 1) \cdot \zeta + (|K_x| + 1) \cdot \xi$$

keys, where, S denotes the storage at node x and $|K_x|$ denotes the size of the key ring at x. The coordinator has higher storage requirements, as it has to store all the key pairs and the corresponding identifiers. Thus, the storage for the coordinator may be sub-classified as: **S**toring Keys and Identifiers: Assuming a pool size P, the coordinator stores the public-private key pair, the master key pair and the list of compromised nodes as

$$CS_1 = 2 \cdot (P + 1) \cdot \zeta + P \cdot \xi + (m + |N_c|) \cdot \alpha,$$

where, $|N_c|$ denotes the number of compromised nodes. **S**toring Merkle Tree Lookup Table: The number of possible permutation for the hash functions is given by: P^2. As the hash function is computed over the key identifier values, it is assumed that the result of the hash function is the same size as the identifiers, i.e. ξ. The result of the hash function serves as the key, while the corresponding key identifiers act as the values in the (key, value) pair.

$$CS_2 = 3 \cdot \xi \cdot P^2.$$

Storing HBP Lookup Table: Assuming a network of size P, each node stores a combination of the key identifiers from the key ring $|K_x|$ at node x. Thus the corresponding lookup table for the coordinator will store the same as values, and map it to the corresponding result obtained from having performed the XOR operation. The coordinator stores

$$CS_3 = \frac{P!}{|K_x|!(P-|K_x|)!} \cdot (|K_x|+1) \cdot \xi$$

keys. Thus, the coordinator requires a storage of (refer Appendix)

$$C = CS_1 + CS_2 + CS_3$$

keys.

Simulation Setup: Connectivity Analysis

As an aid towards analyzing overall network connectivity, we developed a 3-dimensional Python framework which aims to emulate the human form and a set of possible (and most frequent) motions and movements. A network size consisting of 23 nodes (including the coordinator) is considered, all of which adhere to the average dimensions of the human form. We estimate 23 possible deployment points (x, y, z), each aimed to sense and relay different physiological features. The coordinator is placed at the center of the area, near The Center of Gravity is typically located. After each sensor placement point is ergonomically determined, it is assumed that the sensors have been deployed and the network is now active. We then simulate a basic set of human movements, which includes and is not limited to the movement of the limbs, arms, legs, etc; all of which adhere to the 244 degrees of freedom that the human body is capable of supporting.

The framework provides a means to analyze network topology as a result of movement and

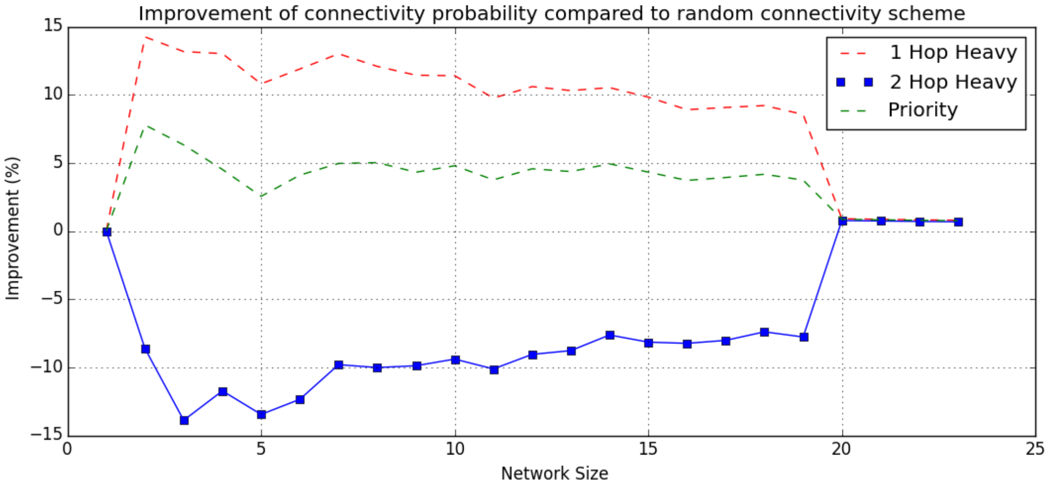

Figure 4.5: Performance of the Different Deployment Schemes with Respect to the Basic Random Pre-Distribution Scheme, Under a Similar Simulation Environment

the distortions produced by the same. Figure 4.4 represents an analysis of how the probability of network connectivity is affected by the pool size (P) and key ring size (K_x), based on key sharing and changing topology, due to the movements. This is similar to the approach adopted by [54], and quantifies how unmitigated network connectivity is influenced by key sharing and unavailability of nodes, across different parameters. Figure 4.5 illustrates how the 2-hop heavy scheme proves to perform worse than the basic random key pre-distribution scheme, and thus is not a suitable rule. Simultaneously, we see that the 1-hop heavy scheme provides an average of 8.74% improvement to the basic scheme while the priority scheme provides an overall improvement of 3.69%. To obtain these results, we evaluated different key distribution rules and compared their performance against the basic scheme in the emulator as mentioned before.

4.5 Motivating Use Cases

To illustrate the usefulness of this work, we discuss possible scenarios where the proposed scheme may be useful for the network. It is critical to take into consideration the physical limitations in a wireless body area network and the design goals that need to be taken into account:

- Provide forward and backward secrecy,
- Low computation cost,
- Low communication overhead,
- Guaranteed key establishment for sensor devices,
- Low storage overhead, and
- Low latency and faster processing.

The proposed scheme aims to provide several computational benefits and an overall enhanced network performance. It allows for improved network connectivity by means of the 1-hop heavy random pre-distribution scheme. Thus, overall, the probability of connectivity is higher and the network topology demonstrates better throughput. The scheme also accounts for compromised nodes and for the compromised keys to be identified, thus allowing for stronger security. Additionally, by means of network re-traceability, it is possible to determine if a node has been compromised. This can be achieved when the coordinator receives an unexpected value for Φ. This implies that the node(s) along that path have been compromised. In such an event, the coordinator may poll the nodes in the WBAN by means of the HeartBeat Package, and identify which nodes have been compromised. The design of a deployment aware key distribution rules maximizes the network performance, and provides better connectivity. By periodically querying the network, it is possible to assimilate a snapshot of the network topology at any instant of time, and to account for network updates and/or modifications. However, the most relevant advantage this scheme provides is an increased network lifetime by means of improved battery conservation. By means of combinatorial optimization techniques, as the one proposed, and by utilizing the 2-hop network topology, WBANs may conserve energy that are traditionally considered as expensive for communication and computation costs.

4.6 Concluding Remarks

While one-way hash functions and symmetric cryptography has its performance benefits, the overall benefits of using PKC outweighs the former. Yet, the use of PKC in sensor networks should be liberal, limited and optimized.

With this research, we have proposed an updated architecture by using public keys in WBAN, which maximizes the benefits of PKCs' but with minimum associated computation complexity. The use of one-way hash functions to authenticate public keys is more cost efficient than performing signature verifications on certificates. Our preliminary results on network connectivity hints towards augmented node resilience capabilities. We see from our initial findings that the proposed scheme exhibits higher levels of safety, privacy, reduced latency and minimizes the standard network overheads.

In our future work, we aim to utilize the network evaluation metrics in a more realistic scenario. The usefulness of the proposed architecture will be investigated using the following metrics: energy consumption, scalability, node resilience, network latency, computation cost and the overall strength of the scheme. As an extension to the proposed scheme, we also aim to investigate the performance when built on-top of the q-composite key distribution scheme. The proposed scheme is easily extensible, and adapts to changing topology and network size. The framework proposed is able to account for several privacy related use-cases and can help combat multiple node compromise scenarios. By maximizing the network properties of WBAN, this framework provides an optimized authentication technique while yielding enhanced security.

Chapter 5

Applying Multivariate Polynomials to WBAN

5.1 Introduction

Wireless Body Area Networks (WBAN) is a special application of wireless sensor networks, designed to facilitate real-time monitoring and reporting of a person's vital signs. WBAN is anticipated to be the next evolution in telemedicine, offering solutions at minimal expense while pushing the boundaries of existing traditional health care. However, defined proposed healthcare sensor network architectures present several challenges of a nontraditional nature as compared to a typical clinical environment. These sensor devices provide limited resources given the reduced processing power and memory constraints, which in turn affect the overall performance. It is desirable that WBAN devices be easy to deploy as they require a user to perform the initial setup and installation (for on-body devices) and should be power efficient and small in size to minimize intrusiveness with body movements.

The likelihood of a targeted adversarial attack for this scenario may be questionable as the consequence from such an attack is severe. The compromise of information in such a medical system may trigger unwarranted actuation, driven by sinister motives. A report issued by the United States Department of Homeland Security highlights upon the vulnerability presented by wearable medical devices, claiming that the relative ease of their hackability by means of targeted malware, has the potential of a "mass murder" [58]. The same sentiments are mirrored by the U.S. Food and Drug Administration Board (FDA) while issuing a warning to all medical device manufacturers, user facilities, hospitals and health care personnel against the high susceptibility of such devices being hacked. This warning was triggered by the work done by white hat hacker Barnaby Jack, who showed that a pacemaker could be disabled, accelerated and made to administer jolts, all within a 50-foot radius.

In this chapter we explore a key sharing and agreement scheme for WBAN(s) to protect them against an outsider. With this research, we aim to create a shared secret amongst the WBAN sensors to ensure integrity and confidentiality. Our focus is to enable a smart key establishment scheme, which performs consistently irrespective of motion and changing topology. Our scheme assumes a WBAN to be a heterogeneous in nature, consisting of devices from various manufacturers which communicate with one local coordinator. Thus, our scheme is equipped to function in a real-world WBAN environment, consisting of both homogeneous and heterogeneous devices, where the devices would not require any extra specialized hardware to ensure secured communication.

5.2 Background and Related Work

Bootstrapping Security in Wireless Sensor Networks

Most of the research in establishing security in wireless sensor networks (WSN) has been with the intention of securing communication when the said technology is deployed on the battlefields. Industrial automation and advent of Internet of Things mandates requirement of designing solutions to cater to the growing needs of establishing security in large scale wireless sensor networks. Confidentiality and trust are the two key components in improving the overall strength of any wireless network, with authentication providing the desired solutions towards enabling necessary access mechanism.

In the case of WSNs, security is typically addressed by means of shared key distribution scheme. However, the more common security solutions in literature are far from being an ideal solution for WSNs [59]. The net effect as dictated by the processing needs, memory requirements, global keying, generic public-key distribution, etc; limit the standard solutions from being useful.

This has led to the design of symmetric key-based solutions specifically for WSNs [54], [60]–[66]. While these solutions are varied in nature, they exhibit wide-scale applicability. Additionally, one approach may be suited for one application, another technique might not be a good solution in such a use. Thus, the overall trade-off between resilience, power consumption and connectivity determines the practicality of a scheme in any given scenario. Researchers have also proposed more context aware schemes, aimed at providing solutions for topology aware network schemes [67]. The latter proved to be more memory efficient and provided better connectivity amongst the sensor nodes.

Research has also shown that certain Public Key Cryptography (PKC) techniques are feasible solutions in WSNs [68], [69]. However, they come at a price. While PKC schemes are scalable and easy to use, authenticating public keys is a computationally costly process and proves to possess a large unnecessary overhead for WSNs.

In this research, we propose a key management scheme for WBAN's. The remaining sections of this chapter describes the scheme and the key considerations that are taken while designing.

Network Model for WBAN

At the lowest level of communication centric to a Wireless Personal Area Network (WPAN) is the Wireless Body Area Network, which follows the IEEE 802.15.6 standards to facilitate communication. It consists of a number of smart nodes, equipped to perform operations such as sampling, sensing, processing and communication of physiological information. Each node (sensor device) directly or by means of two-hop communication communicate with the WBAN local controller, which serves as the sink to this network. By means of the WBAN controller, information is communicated to the Internet or a WPAN. While a WBAN may exhibit multiple topologies, they are primarily restricted to two-hop communication [70].

Key Sharing in WBAN

WBANs can be applied to a wide range of applications, including and not limited to ubiquitous health monitoring and emergency medical services. This covers both long-term monitoring and real-time relay of medical data. Data in transit has to be protected and all security concerns have to be addressed. It is imperative for a WBAN to establish trust amongst the sensor nodes, especially to provide integrity and encryption. However, applying traditional secret key sharing techniques from wireless sensor networks (WSN) proves to be challenging for our use. This is because in WSNs, secret keys are usually pre-distributed before an actual network deployment. A point in consideration is that the WBAN infrastructure may consist of devices being retailed by several different manufacturers, pre-distribution of keys is not the most trust worthy solution for such a heterogeneous network architecture. Additionally, given constantly changing network topology, providing high network connectivity is a challenge. The use of a central key authority is a popular solution for distributing keys in a wired network, however the overhead of the same is not practical in the context of a WSN. Given the deployment scenario and the high demand for usable security, a "plug and play" solution is required which would involve minimal human participation, with a rapid bootstrap process. In our research, we propose a lattice based device pairing protocol with the aim of establishing secret keys within a WBAN. Once, the keys have been established, traditional cryptographic techniques may be applied to generate the shared secret key based on network connectivity at that instant of time. Biometric based security solution is a popular solution towards providing for a security suite in a WBAN. Here, physiological or behavioural information is used for generating and managing the cryptographic keys. Popular biometric techniques include and are not limited to ECG, heart beat, gait, bioimpedence, etc.

5.3 Architecture and Components

Goals and Concerns

Some of the primary concerns that have to be addressed when proposing a key management framework are:

- Storage of key material,
- Distribution of key,
- Revocation and expiration of key material,
- Inspection of key's life cycle, and
- Reporting compromise and events.

In this research, we apply the properties of symmetric multivariate polynomials [71] to grid-based key pre-distribution schemes [72]. This has an added advantage of inherently

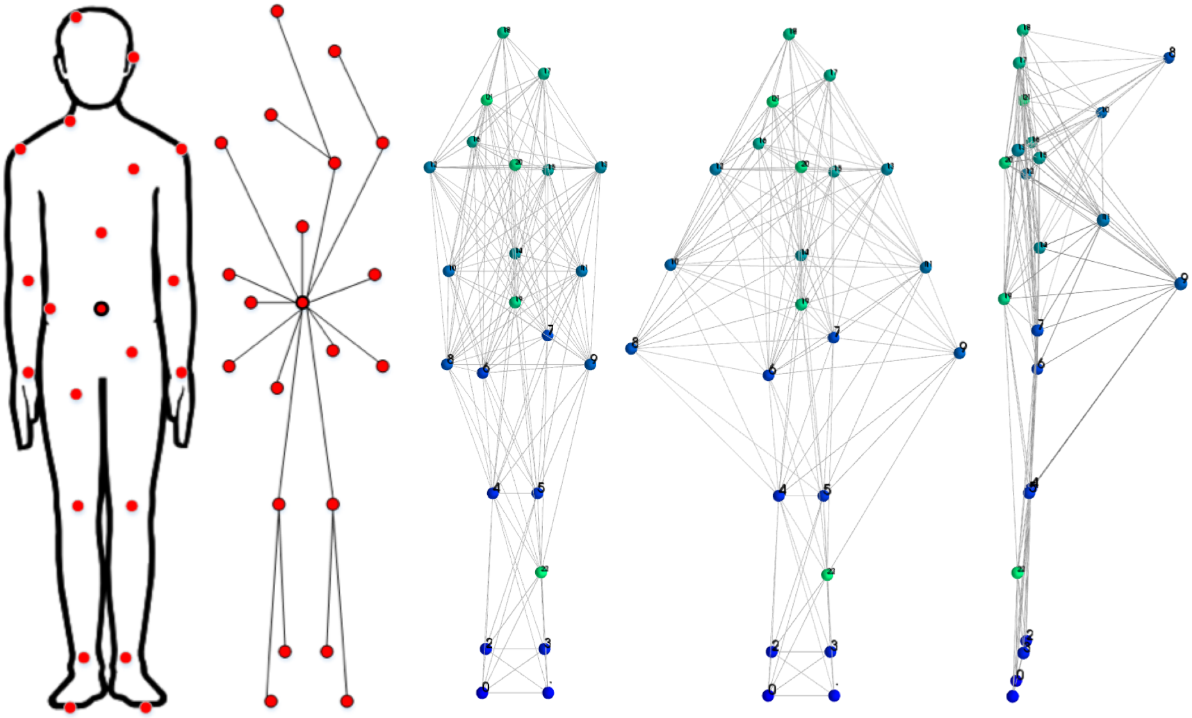

Figure 5.1: Evolution of the Simulator; (L-R) Stage 1: Deploy n nodes across the human frame, Stage 2: Determine the nodes within sensing radius of each node, build tree of links, Stage 3: Determine all possible links between nodes based on keys, Stage 4: Update links based on motion [Front View and Side View]

enabling the intrinsic advantages provided by both schemes, thus providing a robust solution towards facilitating improved connectivity. Here, we do not address the problem of key revocation, and we will do so as we extend this scheme. While we do not audit a key's life cycle, we critique upon the performance of the network when compromised and how the resilience of the network is affected by a node compromise. This research aims to provide a lightweight, rapid key establishment technique between nodes in a WBAN, while providing a high probability of maintaining connectivity.

Deployment Scenario

As per the IEEE 802.15.6 standard, a typical WBAN may consist of up to 256 nodes, with the human body capable of hosting 20 to 50 devices at any instant of time. The number of devices residing on the human frame is highly dynamics, as nodes may be added, replaced or removed at leisure. To test the strength of the proposed system and to evaluate network connectivty, we run a set of simulation studies. For our simulations, we have considered a network capable of having a maximum of 45 nodes. A typical WBAN consists of two types of nodes (with respect to the local coordinator): static and dynamic. A static node is one which is typically located at a fixed distance from the coordinator, thereby they form a static network topology centric to the coordinator (such a heart rate monitor). A dynamic topology is formed by the sensors which are typically located on the extremities of the human frame, such as arms and legs. This hybrid network topology proves to be a challenge when designing security solutions. Additionally, WBANs are typically designed to form a star topology, with sensors being either 1 hop or 2 hop away from the local coordinator located at the centre. To test the performance of our scheme in a real-world scenario, we also emulated a wide range of human movements and analyze the performance of our scheme during the same (Figure 5.1). The emulator embodies a framework which supports 23 strategically located sensing points (including the coordinator). Later sections highlight upon the specifics behind the simulator design concerns. The simulation framework is built upon Python, integrating scientific computational modelling with data visualization and 3-D rendering. It supports emulation of human movements in 3 dimensional space and is capable of modelling all 244 degrees of freedom that the human body is normally capable of performing.

Grid-Based Polynomial Key Distribution

Seeking inspiration from the probabilistic random key pre-distribution scheme, *grid-based* key pre-distribution is another popular technique used for establishing secure communication in WSNs. For a 2 dimension grid, assume that N sensor nodes have been deployed. The grid-based polynomial scheme then builds a $m\ x\ m$ grid consisting of 2m polynomials $f_i^c(x, y), f_i^r(x, y)_{i=0,...,m-1}$, where $m = |\sqrt{N}|$. Here, each row (i) and each column (j) is associated with a polynomial $f_i^c(x, y)$ (Figure 5.2). Each sensor is assigned a unique intersection in this grid; such that for the sensor node located at (i, j), the polynomials held are $f_i^c(x, y)$ and $f_i^r(x, y)$. Using this information, shared key discovery and key path establishment in facilitated. Here, instead of storing an extra node ID, the sensor's coordinates are used to generate its corresponding node ID. Thus, for the sensor at (i, j), the node ID can be generated by concatenating the row and column to yield $\langle i, j \rangle$. Such a scheme has several benefits, including and not limited to, improved network connectivity and strong resilience to node compromise. Lastly, this scheme shows all the benefits of the polynomial based pairwise key sharing scheme with minimal communication overhead for shared key discovery. For our scheme, we are interested in a 3 dimensional grid, aimed at providing key sharing using multivariate polynomials [73].

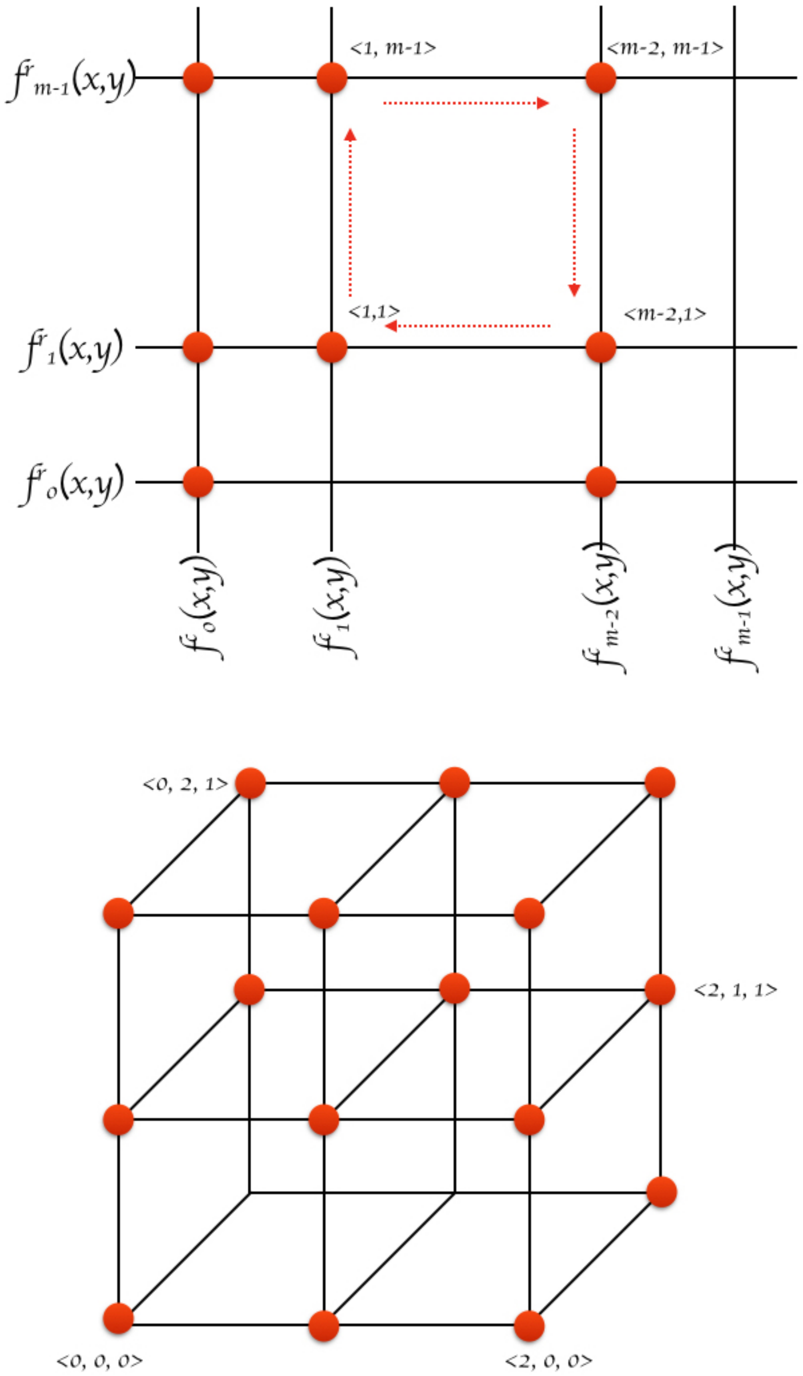

Figure 5.2: Visualization of the Grid

Attack Model

Before we introduce our solution, it is important that we also address the nature of the attacks and the possible scenarios that leads to a compromise state. Here, we are concerned with how challenging it is to establish pairwise keys between two sensor nodes. Additionally, we study sensor node compromise under specific circumstances, that is after a sensor node has already been captured.

Hypothetically, if two sensor nodes s_i and s_j wish to communicate, the only way the communication between them may be jeopardized is by compromising the shared polynomial between them. Assuming that l-degree polynomials are distributed at each sensor, this would require that atleast $l + 1$ nodes would have to be compromised. Additionally, assuming that even if $l + 1$ nodes are compromised, the nodes may still be able to establish a link by means of alternate paths. In the case of nodes which wish to determine a pairwise key by means of path key establishment; if the attacker successfully compromises even one of the sensor required to establish the pairwise key, and lands the message being relayed between the two nodes, they may now determine the shared key. If however the compromised node is identified, the nodes try to establish communication using alternate paths. As such, the attacker would be required to prevent (or block) the communication between all the sensor nodes connected to s_i and s_j. Thus, this implies that, to avert pairwise key establishment, the attacker would be required to compromise atleast one sensor node along each possible path.

Another scenario presents itself wherein an attacker may choose to randomly compromise sensor nodes in a WBAN. This is usually done to compromise the path discovery process, thereby increase the overall system latency by making the process of establishing pairwise keys more challenging. If we assume that p_c sensor nodes have been compromised, and there are $m \times n \times o$ sensor nodes deployed, the probability that η shares on a particular multivariate polynomial has been compromised is given by:

$$P(\eta) = \frac{(m \times n \times o)!}{\eta!((m \times n \times o) - \eta)!} p_c^{\eta}(1 - p_c)^{m-\eta}$$

Consequently, probability that 1 multivariate polynomial is being compromised is given by $P_c = 1 - \sum_{i=0}^{t} P(i)$. In case of two non-compromised sensor nodes which do not have any compromised polynomial share, the probability that a pairwise key between them may be compromised is given by $(1 - \frac{3(m \times n \times o - 1)}{\Delta - 1}) \times p_c \approx p_c$, where Δ is the maximum sensor nodes in the network. Such sensors are incapable of establishing a shared secret key directly, and action nodes between them are rendered compromised. As a result of this, these sensor nodes are unable to communicate. As a part of the design consideration, it is important to account for messages in transit. Attackers may eavesdrop upon messages, encrypted or unencrypted, while they are relayed between sensor nodes through air. Also, while it has been suggested that tamper-resistant hardware might provide an added security level, this solution is not fool-proof.

5.4 Design Details

This section details the design of the proposed scheme and how it aims to satisfy the requirements as stated before. This section details on our design discussion and how our protocol serves to provide higher network connectivity, while keeping memory costs at a minimum. The proposed scheme consists of three phases: *share pre-distribution, direct key calculation* and *indirect key negotiation.*

Constructing the Lattice

As per the IEEE 802.15.6 standard, three security levels have been defined, namely Levels 0, 1 and 2. Every node and coordinator in a WBAN has to satisfy the stages at the MAC layer before data exchange may be enabled (Figure 5.3). Every node in a WBAN is initially in an *Orphan* state. What this implies is that the device does not have any relationship with the local coordinator, as a result of which it remains untethered. Once the device establish a secure association, the node now enters the *Associated* state. During the association phase, a pre-shared master key (MK) is activated and a pairwise temporal key (PTK) is created. Usually, the master key is distributed using Level 0 (unsecured communication level). At the *Secured* state, the nodes are now connected to the local coordinator and may exchange frames securely.

As described before, a 3 dimensional grid (referred to as the lattice) is considered. Here, the lattice takes up a $m \times n \times o$ vector space, where $m, n, o = (2k + 1)$, for any $k \in N$ and

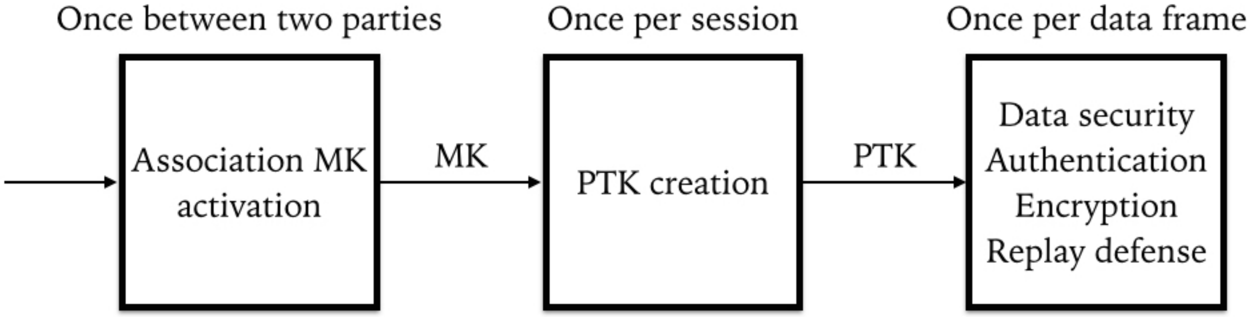

Figure 5.3: Phases of Key Generation

$n > m \geq o$. Also, $|m \times n \times o| = \Delta$, where Δ denotes the maximum number of sensor nodes in the network. In this research, we assume that the local coordinator will serve as the gateway to the outside world. For such reasons, we assume that the coordinator will always be available and remain uncompromised throughout its lifetime. With digital wallets now becoming a reality, we can assume that the typical smartphone is capable of being able to hold onto critical user data while retaining user integrity. In this architecture, similar to a grid-based key distribution scheme, we assume that the coordinator is the setup server and is relatively secure. The coordinator has been designed such that it is aware of the possible sensor based devices that may communicate with it, and how they are spread out across the human frame (invasive and non-invasive). For example, suppose user X has been diagnosed with Heart Rate Variability (HRV) and has been advised to wear a 24*7 heart rate monitoring system. Possible sensing areas for heart rate measurement is fixed on the human frame, with a chest strap being the most popular candidate from the available options. Given that the point of measurement is fixed, and the relative distance of the device and the coordinator is nearly static, we can assume that the device shall always be mounted on the left side of the chest. Similarly, EEG, ECG, cochlear implants, fitness devices, EMG devices, etc; all have relatively fixed sensing points on the human form, thus we can estimate their coordinates beforehand. What this implies is that, given the possible sensing points, and nodes that can be mounted on the said points, we have a fixed coordinate system that can be mapped onto a 3-D coordinate plane. Assuming the orthostatic position to be the initial deployment state for the sensing devices, we may now construct a lattice around it.

Traditionally, the coordinator is assumed to be either a Personal Digital Assistant (PDA) or a smartphone, both of which are usually placed around the pelvic region. Given the uncertainty in the optimal placement of the coordinator, we assume that it may be located anywhere or in the near vicinity of the pelvic region. To increase the probability of establishing communication with the coordinator, and for improved fault tolerance in the presence of compromised nodes, we recommend building multiple paths to the coordinator. Consider a network of size Δ nodes, that is mapped to the aforementioned lattice which has a *x, y and z* axis. The columns of the different dimensions are denoted by $\kappa_x, \kappa_y, \kappa_z$. As sensor nodes are introduced into the network, they are assigned a unique intersection on the grid. Thus, each sensor node is associated with a 3 axis coordinate of the form $\langle \kappa_x, \kappa_y, \kappa_z \rangle$. Additionally, each axis in the lattice is assigned a symmetric polynomial, such that all sensors along a single axis share atleast one polynomial.

Key Agreement Model

To establish key agreement between any two sensors, we propose that each axis of the lattice be associated with a l-degree trivariate symmetric polynomial, as defined by:

$$f(x_1, x_2, x_3) = \sum_{i_1=0}^{t} \sum_{i_2=0}^{t} \sum_{i_3=0}^{t} a_{i_1,i_2,i_3} x_1^{i_1} x_2^{i_2} x_3^{i_3}. \tag{5.1}$$

Where the coefficient of a polynomial is chosen from a finite field $\mathbb{F}_q$, here q represents a large prime capable of accommodating a cryptographic key. All calculations are performed over the finite field $\mathbb{F}_q$. A three dimensional ordered pair is defined as a bijective mapping

$$\sigma = \{1, 2, 3\} \rightarrow \{1, 2, 3\}. \tag{5.2}$$

The coefficients are determined based on the available selection from:

$$a_{i_1 i_2 i_3} = a_{i_{\sigma(1)} i_{\sigma(2)} i_{\sigma(3)}}.$$

By permuting over σ of $\{1, 2, 3\}$, a symmetric polynomial is obtained such that:

$$f(x_1, x_2, x_3) = f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}),$$

For every node deployed, it should have atleast two credentials in common with another sensor node, and they should be *positive* and *pairwise different*. For any two sensor nodes s_i and s_j that have IDs such that $i = \langle \kappa_x || \kappa_y || \kappa_z \rangle$,$j = \langle \kappa_x || \kappa_y || \kappa_z \rangle$, if $i \cdot \kappa_x = j \cdot \kappa_x$ or $i \cdot \kappa_y = j \cdot \kappa_y$ or $i \cdot \kappa_z = j \cdot \kappa_z$; it implies that the sensor nodes s_i and s_j share atleast one common dimension and a shared polynomial. Thus, the polynomials $f(s_{i_{\kappa x}}, s_{i_{\kappa y}}, \kappa_z)$ and $f(s_{j_{\kappa x}}, s_{j_{\kappa y}}, \kappa_z)$ are loaded into the sensor nodes. In this case, the coefficients of the two polynomials are loaded into the memory of the sensor nodes, rather than the polynomial itself. If $s_{i_{\kappa x}} = s_{j_{\kappa x}}$ or $s_{i_{\kappa y}} = s_{j_{\kappa y}}$, then sensor nodes s_i and s_j may compute a shared key as:

$$K_{s_i s_j} = f(s_{i_{\kappa x}}, s_{i_{\kappa y}}, \kappa_z) = f(s_{j_{\kappa x}}, s_{j_{\kappa y}}, \kappa_z),$$

where κ_z is the common credential between the two nodes.

Taking cue from the 802.15.6 standards, during device enrollment, a device is in an orphan state and seeks to establish a relationship with the coordinator. Once the coordinator receives this request, it determines the nature of the device and its possible sensing zone and accordingly it allocates the node a unique intersection in the lattice. This may be based on the exact location pinpoint of the device, or if the device is within a region where in it maintains a Hamming distance 1 from its projected sensing point. Once the device is associated with a coordinator, it receives its coordinates and the associated polynomials. Collectively, they function as the Master Key (MK) and may be induced to generate the TPK (temporal pairwise key) during communication. Typically, node credential information is relayed over the unsecured communication channel (Level 0) and may be done using Over-The-Air (OTA) technology, or by physically plugging the device into the coordinator over serial connection.

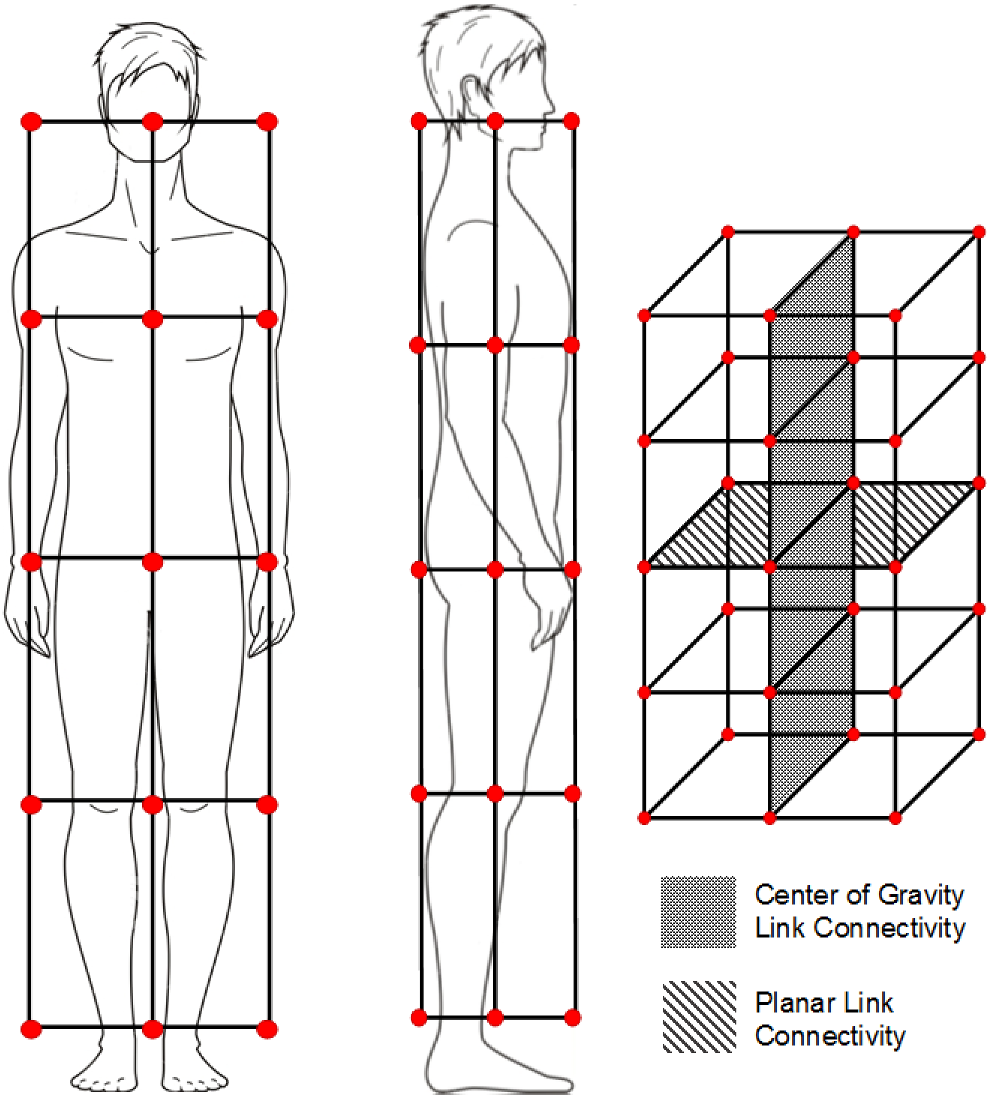

Figure 5.4: Building the Lattice with Respect to the Human Form

Coordinator Link Connectivity

The aim of this research is to account for fault tolerance and improve the overall network connectivity, in the event of a node compromise. As mentioned earlier, the location of the coordinator is only known approximately and the exact location depends upon user preference. Taking into consideration the static-yet-dynamic nature of the network model, the goal is to improve deterministic key agreement between any pair of nodes, while ensuring that the hop count remains a maximum of 2. We assume that the coordinator is capable of greater memory store than the other nodes and has greater processing power. Each node stores $d \times f(x_1, x_2, x_3)$ polynomials, assuming it has d immediate neighbors which are at a Hamming distance of 1. In addition to this, before a network is deployed, a global l-degree tri-variate polynomial is selected. The same polynomial is reused to derive polynomial shares for all associated nodes. However, the coordinator follows a different assignment and connectivity scheme (Figure 5.4).

Planar Link Connectivity (PLC)

Under this case, the coordinator is assumed to be located anywhere along the pelvic region of the human frame. As the placement of this device may vary about a particular axis, we load all the keys for these sensors into the coordinator. Assuming the same lattice $m \times n \times o$ as before, the coordinator stores the IDs of the nodes that satisfy the condition $(x_{col}, y_{median}, z_{aisle})$, where $col = 0, ..., m$ and $aisle = 0, ..., o$. The coordinator also stores the polynomials:

$$\begin{aligned} f(x_1, x_2, x_3) &= f(x_1^{i_1}, x_2^{median}, x_3^{i_3}) \\ &= \sum_{i_1=0}^{t} \sum_{i_2=0}^{t} \sum_{i_3=0}^{t} a_{i_1,i_2,i_3} x_1^{i_1} x_2^{median} x_3^{i_3}. \end{aligned}$$

Center of Gravity Link Connectivity (CGLC)

The Center of Gravity (CoG) is defined as the midpoint or center of the weight of a body or an object. On an average, the center of gravity in an adult human frame is in the mid-pelvic cavity. Research has shown that the optimal placement for the coordinator is towards the center of the body [74]. In the 802.15.6 standard, WBAN transmissions are possible across three different channels, namely Narrowband (NB), Ultra-wideband (UWB), and Human Body Communications (HBC). Similar to the lattice in the aforementioned scenario, the coordinator stores the IDs of all the nodes that satisfy the condition $(x_{col}, y_{row}, z_{median})$, where $col = 0, ..., m$ and $row = 0, ..., n$. The coordinator also stores the polynomials:

$$\begin{aligned} f(x_1, x_2, x_3) &= f(x_1^{i_1}, x_2^{i_2}, x_3^{median}) \\ &= \sum_{i_1=0}^{t} \sum_{i_2=0}^{t} \sum_{i_3=0}^{t} a_{i_1,i_2,i_3} x_1^{i_1} x_2^{i_2} x_3^{median}. \end{aligned}$$

Direct Key Establishment

Similar to Grid-based Polynomial Key Distribution, two sensor nodes may establish a shared key directly if they have an identifier in common, i.e., a common node index in their

IDs. However, in this scheme, for two sensor nodes to communicate, they need to share atleast 2 credentials amongst themselves to facilitate key sharing. Typically, two sensor nodes are guaranteed to share minimum two credentials if they have a Hamming distance of exactly 1. The sensor nodes determine if they share credentials from the node IDs, which they share between themselves. Having determined which credentials align, the sensor nodes now determine which polynomial to use to compute the mutual key.

Determination and computation of a mutual key is independent of any interaction with the other logical neighbors. The key used to encrypt and decrypt the information between the neighboring nodes is secret, known only to them. An adversary is privy to such information only if they are aware of the polynomial against which the sensor nodes communicate.

Indirect Key Establishment

If in case two sensor nodes share one or no common credentials between themselves, they establish connectivity using an intermediate sensor node. This is possible when the two sensor nodes reside in different planes. Suppose two sensor nodes s_i and s_j need to establish a shared secret, with i, j as identifiers. The two sensor nodes pick an intermediate sensor node, known as the *agent* sensor node to act as the connection facilitator between them. Thus, the sensor nodes in the nearby vicinity serves as the agent, such as s_ϕ. Here, ϕ is the identifier which satisfies one of the following:

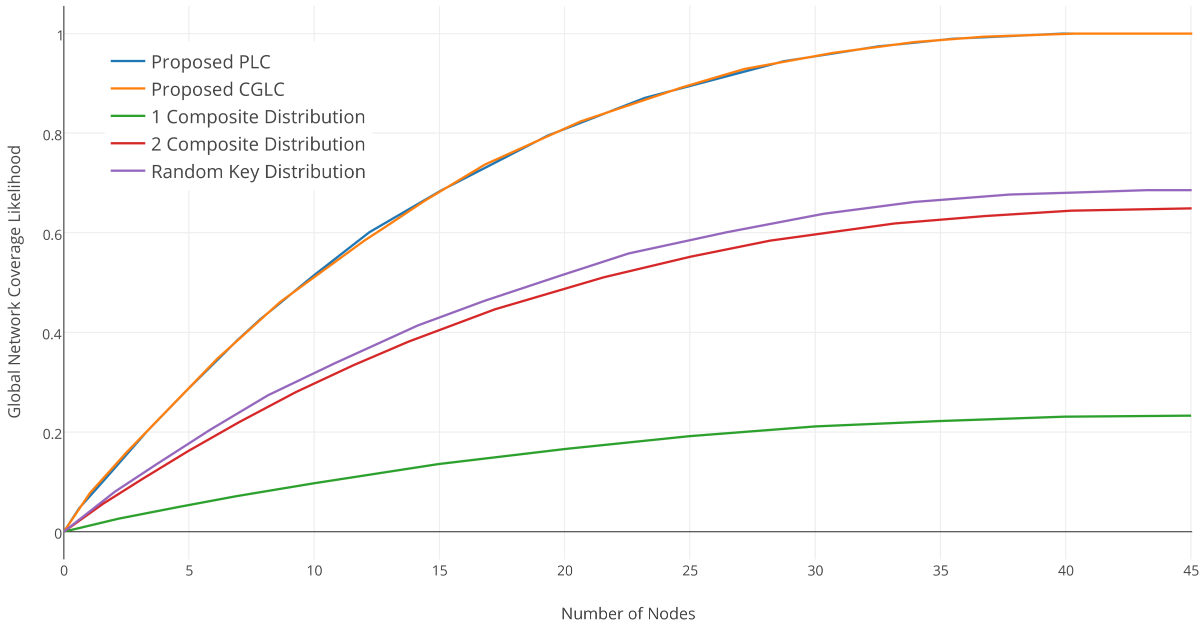

Figure 5.5: Lattice-Based Evaluation of Network Connectivity

$$\begin{aligned}\phi\cdot\kappa_x = i\cdot\kappa_x\,and\,\phi\cdot\kappa_y\,and\,j\cdot\kappa_y\,or\,\phi\cdot\kappa_z = j\cdot\kappa_z,\\ \phi\cdot\kappa_y = i\cdot\kappa_y\,and\,\phi\cdot\kappa_x\,and\,j\cdot\kappa_x\,or\,\phi\cdot\kappa_z = j\cdot\kappa_z,\,and\\ \phi\cdot\kappa_z = i\cdot\kappa_z\,and\,\phi\cdot\kappa_x\,and\,j\cdot\kappa_x\,or\,\phi\cdot\kappa_y = j\cdot\kappa_y.\end{aligned} \tag{5.3}$$

Based on common credentials, the corresponding share of ϕ is used to render the node s_ϕ as an agent. Thus, by means of computing $K_{s_i\phi}$ and $K_{\phi s_j}$, key shares between s_i and ϕ and s_j and ϕ are determined. This helps resolve the problem of indirect key negotiation.

5.5 Path Finding and Connectivity Assessment

A wireless BAN takes departure from a traditional WSN in that the network size is smaller and more dense in distribution. When two sensor nodes are direct neighbors, they may exchange keys using the polynomial they share between themselves. Thus, this enables them to establish keys directly rather than having to seek an intermediate neighboring device.

Connectivity

Connectivity is defined by the number of sensor nodes that can continue to establish communication based on the original keying material assigned to them. Let $\alpha = \sqrt[3]{mno}$, thus the overall connectivity in the scheme is given by $3 \times \dfrac{\alpha^2 - 1}{\alpha^3 - 1}$ when connectivity is limited to a single hop. This approximates to $\dfrac{3}{\alpha + 1}$. For cases where the hop count is limited to a maximum of 2-hops from the target, the overall connectivity is given by:

$$C_{conn} = 3 \times (\frac{\alpha - 1}{\alpha^3 - 1}) + hp(v) = \frac{3}{\alpha^2 + \alpha + 1} + hp(v).$$

Here, $hp(v)$ refers to the set $\{s_i | s_i \longleftrightarrow s_j\}$. To analyze the performance of our scheme, we use the basic scheme [54] and the q-composite scheme [66] as comparison metrics. We evaluate our scheme against their performance under similar conditions.

Eschenauer and Gilgor [54] proposed a simple protocol, which enabled effective concession between scalability and robustness. In this proposed scheme, a large key pool is generated and random k keys are assigned to each sensor node, thus forming a key ring. For two

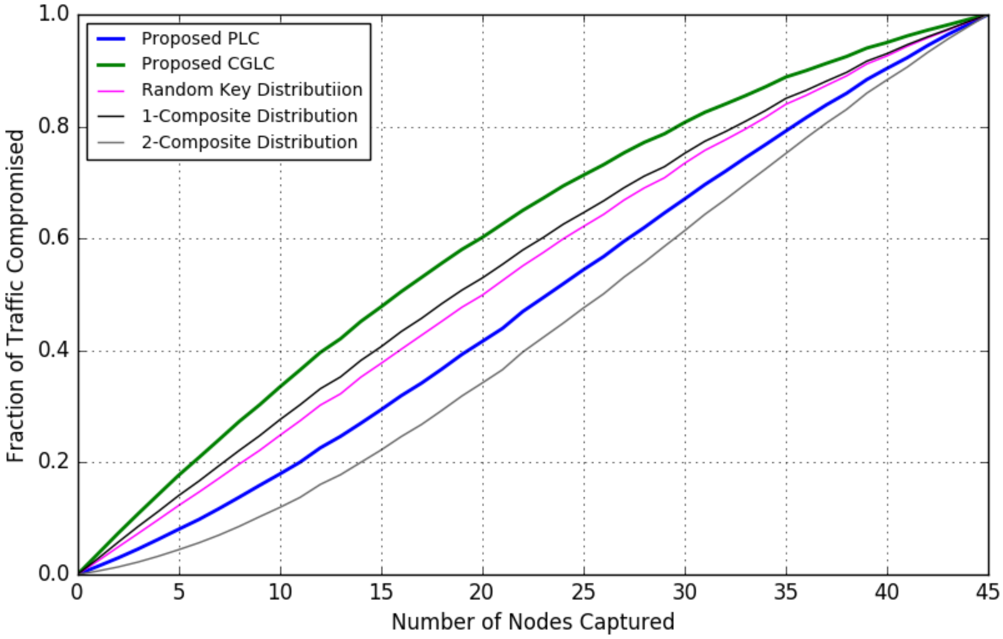

Figure 5.6: Lattice-Based Evaluation of Connectivity, Given Node Compromise

nodes to communicate, they would be needed to share and establish a common key between themselves. The biggest disadvantage of this scheme is that it lacks an authentication process and does not ensure connectivity between deployed sensor nodes, thus some nodes might be unreachable given the random nature of key assignment. Additionally, while the scheme does not account for collaborative operations, it is extremely scalable. The q-composite scheme is similar to this, the only difference is that two nodes would require q keys to be able to communicate between themselves.

In our simulation environment, the key ring has been defined to be of size 3 ($k = 3$). This is in keeping with the tri-variate polynomial scheme that has been applied as a part of the proposed framework. Here, the size of the key pool is fixed at 11. With the parameters as mentioned before, the network model is executed and the performance of the proposed scheme is evaluated.

Simple Grid-Based Evaluation

The simple grid based topology evaluates connectivity of the sensor nodes when deployed as a $5 \times 3 \times 3$ lattice, for both PLC and CGLC. This evaluates connectivity at the logical node level, as they reside on the coordinator, before its deployed at the device level (Figure 5.6). In the simulation environment, we analyze connectivity for 45 nodes (Figure 5.5). Here, the connectivity based on external network attack is also addressed; and the performance for a compromised network is evaluated. Figure 5.6 depicts that a higher percentage of a network is available using alternate paths even after a node has been compromised in the proposed PLC scheme.

Kinesiology-based Connectivity

We evaluate the performance of our scheme for a real-world deployment. To do this, we simulate our proposed scheme for a wide set of human movements and actions, and evaluate how the connectivity is affected by motion (Figure 5.7). We also simulate for compromised nodes, and evaluate how PLC and CGLC performs under similar conditions, as mentioned before (Figure 5.8). This is done with the intention of testing the network strength and performance, based on external attacks.

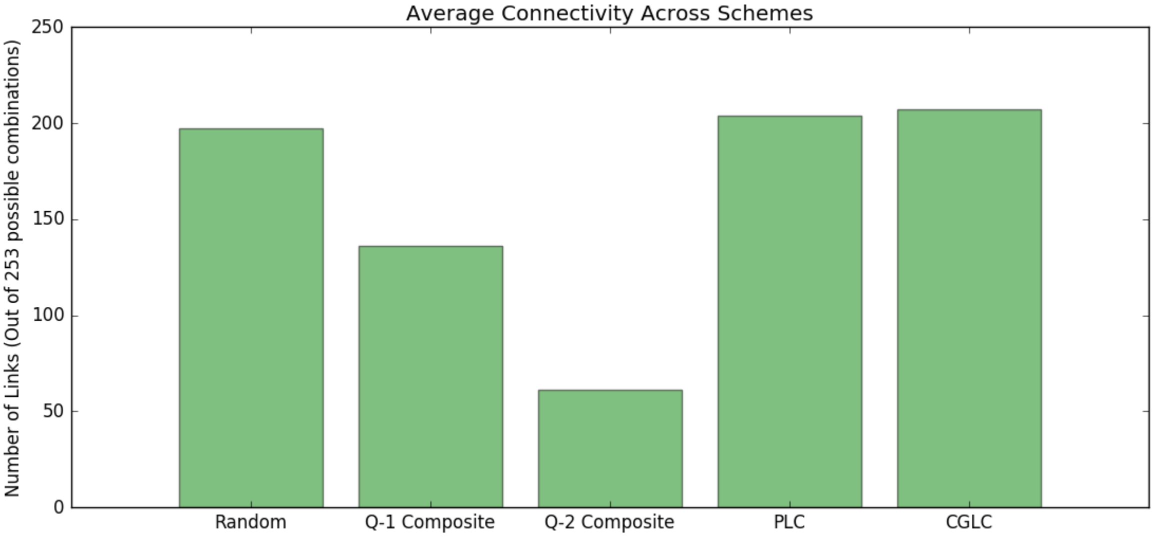

Figure 5.7: Average connectivity

Computation Overhead

The total computation cycles required for information relay is determined by whether two nodes can compute a mutual key or not. By computing $f_R(n)$, it is possible to determine the average running time for computations in the network system. To establish keys between two sensor nodes that form a direct path, the computation requirements mounts to $C_{directPairs} = 2t - 3$ multiplications, to evaluate a polynomial of the order of l. To compute the computation cycles required to establish a path between indirectly connected nodes is given by

$$C_{indirectPairs} = C_{directPairs} \sum_{i=1}^{n} i f_R(i).$$

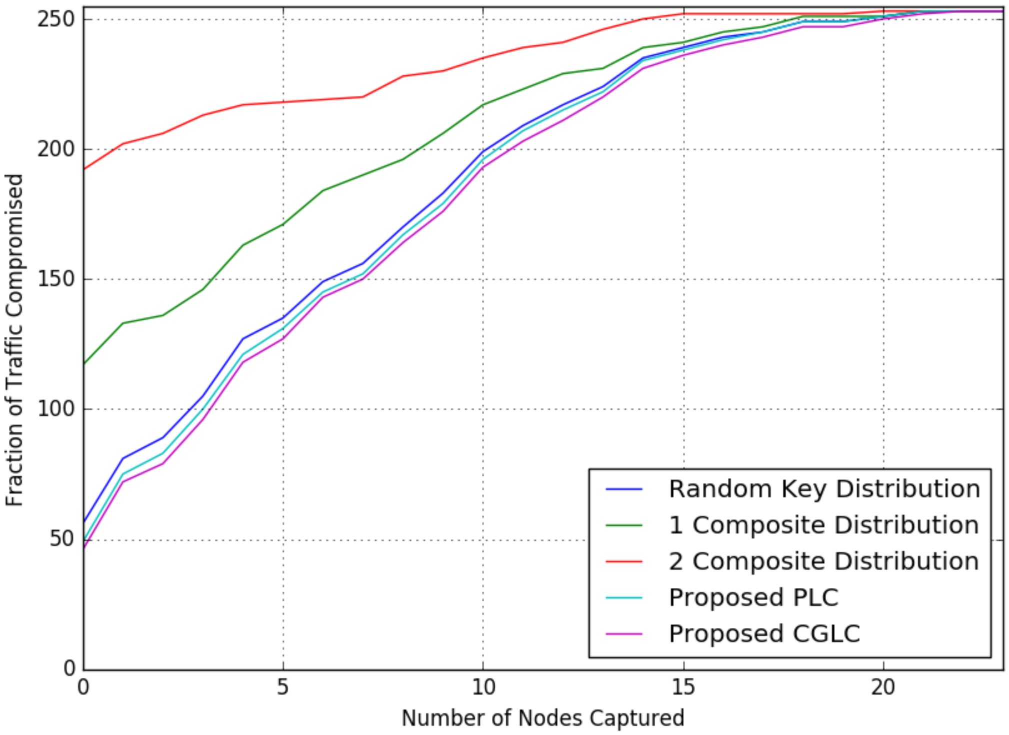

Figure 5.8: Network Availability given Node Capture

Memory Overhead

All the nodes defined in the WBAN topology hold a partial l-degree trivariate polynomial, by which a shared key is established. Thus, the power of l directly affects the storage requirements of each sensor node. Traditionally, the memory store has two parts, the first stores the sensor node ID and coefficients of the polynomials it uses to establish the shared key, while the second stores the sensor nodes that have been compromised, such that connection to them is avoided. The memory required for the nodes is given by:

$$S = 3[(t+1)log_2(Q)] + 3(N_c+1)\lceil log_2(m \times n \times o)\rceil. \tag{5.4}$$

Here, S represents the memory required per node, $log_2(Q)$ is the memory required to store the l-degree polynomial at each node, such that it may be reconstructed appropriately. Finally, N_c refers to the number of compromised nodes.

Communication Overhead

One of the key requirements in any WSN is to keep the communication overhead at a minimum. This includes and is not limited to the key exchanges between the two sensor node identifiers. As established before, path discovery could be by means of direct keys or through intermediate nodes. In general, exchange of identifiers may be represented by $log_2(m \times n \times o)$ bits. In order to exchange IDs between 2 nodes, the number of bits required is given by

$$CO_{avg} = \frac{1+2}{2} \times 3\lceil log_2 \sqrt[3]{mno}\rceil. \tag{5.5}$$

In a more real-world implementation, taking into consideration communication traffic and its associated costs, communication overhead is defined by:

$$CO_{avg_p} = 3\lceil log_2 \sqrt[3]{mno}\rceil \sum_{i=1}^{n} if_R(i). \tag{5.6}$$

Effect on the Network Topology

It may be possible that two sensor nodes do not share a key between themselves during the shared-key discovery phase. This implies that with respect to the network router (in this case, the coordinator), the two nodes do not share a common link between themselves. In totality this affects the average path length and connectivity between nodes after shared-key discovery. Given that some nodes may not be directly reachable, a multi-link path may be required to reach a specific node. It is desirable to have the path short, as longer path lengths imply increased communication overheads, increased latency and transmission costs. Figure 5.9 depicts how the overlap factor differs across the scheme. We define overlap factor as the average number of possible links that may exist between two nodes. In simple terms, this is the average number of keys two nodes may share between themselves to establish communication.

By studying the link connectivity across each node, one might reason that it might be possible to determine the critical sensor nodes based on average network connectivity. Critical sensor nodes are those sensor nodes which serve as local gateway points to the other nodes in the network, or those sensor nodes which might serve as natural cluster heads. However, given the dynamic nature of the network topology and stochastic property of link connectivity, the overlap factor varies across the sensor nodes. As the overlap changes, we can conclude that the average number of links across nodes is consequently updated. Therefore, the identity of the critical nodes is not compromised and remains a secret to third-party observers.

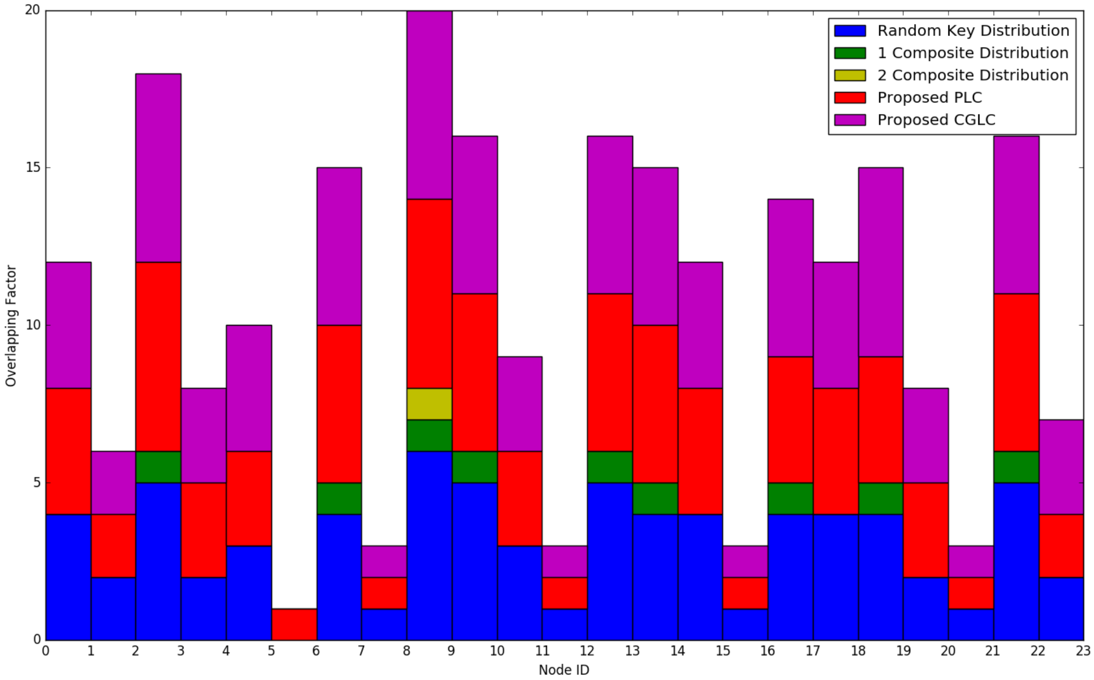

Figure 5.9: Variance of Overlap Factor across Schemes

Resilience Against Node Compromise

Evaluation of the resilience of the proposed scheme may be performed by determining what percentage of the network remains susceptible to compromise, given a compromise (other than the coordinator) has already occurred. A key design in this scheme is the ordered distribution of the keys amongst the sensing nodes. As mentioned earlier, if the shared polynomial is known by an external attacker, then the corresponding keys may be deciphered.

Assume P is the polynomial being used between a pair of sensor nodes to establish a key between themselves. When a third sensor node, other than these two specific sensor nodes is compromised, the probability that P will not be compromised is given by:

$$1 - \frac{t}{|N|}.$$

Here, t refers to the number of polynomials stored by each sensor node (in this case, $t = 3$) and /*N*/ refers to the total number of polynomials defined. Given, x nodes are compromised, the probability that P will not be compromised is given by:

$$(1 - \frac{t}{|N|})^x.$$

This implies that, the total number of keys being compromised may be estimated by:

$$1 - (1 - \frac{t}{|N|})^x.$$

The results obtained from the analysis as depicted above show that the proposed scheme performs better than the more traditional key distribution schemes. It lowers the fraction of compromised communication links after an event of compromise has already occurred.

5.6 Conclusion

This proposed research utilizes a hypercube inspired multivariate polynomial scheme to establish pairwise keys in a Wireless Body Area Network. Here, a multidimensional grid was mapped onto a human frame, such that each sensing point may be modelled as an intersection in the grid, leading to the formation of the resultant multivariate polynomials. As per the design of the scheme, a pair of sensor nodes would be required to be at a Hamming distance of 1 to be able to establish direct keys between them. In the event that a direct key may not be established, the two nodes would establish a key path between themselves using an intermediate sensor node. The main advantage of this scheme is that it improves the overall global connectivity of the network and increases the probability of a tertiary or secondary node's communication likelihood with the coordinator. An analysis of the simulation results show that the proposed scheme provides significant improvements over other existing similar schemes.

The proposed scheme is easily extensible, and adapts to changing topology and network size. The framework proposed is able to account for several privacy related use-cases and can help combat multiple node compromise scenarios. By maximizing the network properties of WBAN, this framework provides a scalable solution towards designing a robust security suite.

Chapter 6

Measuring the Authenticity of Vehicular Infrastructure

6.1 Introduction

Advanced Driver Assistance Systems (ADAS) came into conception as a means of providing increased driver safety and works by sensing the immediate surroundings of a vehicle in motion, and interpreting those findings to trigger the corresponding actions. Recently, driver assistance systems have been known to incorporate Intelligent Speed Adaptation (ISA) as a solution to concerns of speeding. Typical ISA system uses one of four possible techniques to determine the permissible speed limit at any instant of time. These are: (a) GPS (Global Positioning Systems) data, (b) Radio beacons, (c) Optical recognition systems, and (d) Dead reckoning. Of these, ISA systems that use GPS data for decision making prove to be the most economically feasible option, for all it needs is an additional GPS receiver. The ISA system is able to determine the physical location of the vehicle, and by looking up the database against the same, determine the local speed limit for that area.

As vehicles become more sophisticated and anti-theft technologies become smarter, stealing them becomes a more challenging ordeal. While some attackers and thieves revert to innovative new methods, others are resorting to still more classic techniques, such as carjacking. Carjacking is one of the least complex techniques on compromising a vehicle. It involves overpowering the car owner and taking control of the vehicle. This two step process is sufficient in overtaking control of almost any vehicle, all this without having to circumvent any sophisticated security features.

Physical security is another facet of this technology, which coupled with software security render the entire infrastructure to be deemed highly critical. Masquerading and providing false information is another means of duping these vehicles, thereby facilitating carjacking. It is possible for an attacker to place a stop sign at an arbitrary location, thereby forcing the vehicle to stop, leading to a scenario where the car may be physically compromised. In addition to this, by way of placing false signs along a road way, it is possible for attackers to pigeon-hole vehicles in dead ends and isolated junctions, thus leading to possible compromise.

Driver safety has been greatly affected by the enabling of technologies that provide detection and recognition of traffic signs. Yet, there are several challenges to be overcome along the way. Tracking objects in a continuous image sequence, based on inputs captured from a vehicle moving at an irregular motion is a challenging problem by itself. However, it is made worse when parameters such as bad weather and air pollution, which reduce visibility, are factored in. In addition to those, variance in lighting conditions due to day and night transitions also affect the gradient of the perceived road sign. All this and more render the design and implementation of recognition systems to be a hard problem, with reliability being a genuine concern. This leads to the need to classify the level of confidence associated with traffic fixtures (such as road signs) and a means to validate their presence; thus appropriately blocking or challenging suspicious activities.

Our contribution. This work provides a novel architecture aimed towards classifying the legitimacy of road side fixtures, termed as *ground truth.* This work is geared towards promoting a "secrecy by design" paradigm, where the end goal is to quantify the secrecy of the classifier irrespective of the strength of its design. Applying the knowledge gained from *adversarial machine learning*, it is possible to strengthened the behaviour of the classifier itself, without having to compromise on its design.

In particular, our contributions are as follows:

- A statistical framework aimed towards identifying suspicious road signage has been proposed. This is done by means of a likelihood ratio test, capable of handling most data types including sparse data sets. The proposed framework is capable of achieving improved accuracy by applying a logistic regression model on the features of the proposed formula 6.7.
- To validate the strength of the proposed system, a prototype implementation has been

developed. The strength of this system is in its capability of accounting for cases wherein new data presents itself, such as new roadside establishments or fixtures. The proposed system incorporates properties such as large-scalability and is supported by an intuition engine which applies geographic information systems (GIS) as its backbone.

- The proposed system has been validated, and its findings reported. To facilitate this, samples from real road testing routes have been used for evaluation in Cincinnati, OH.
- Taking into account the models developed by adversarial machine learning techniques, an attempt has been made to classify potential attacks against the classifiers. By hypothesizing probable attack scenarios and by simulating potential attacks, the effectiveness of the attackers attempting to evade the classifiers have been evaluated.

This work can in principle be applied to any standing authentication system, and in theory support any hard authentication system, before the vehicle attempts to implement the instructions being advised by the regulatory sign (RS).

Experimentation

As a proof-of-concept implementation, the study was performed using stop signs, but in theory, the same concept may be applied to a wide range of regulatory signs. To evaluate the performance of the proposed architecture and its application, a series of road trials (approximately 750 rounds) were conducted along a fixed route in Cincinnati, Ohio, U.S., as depicted in Figure 6.1. This data included approximately 190,000 data points, of which

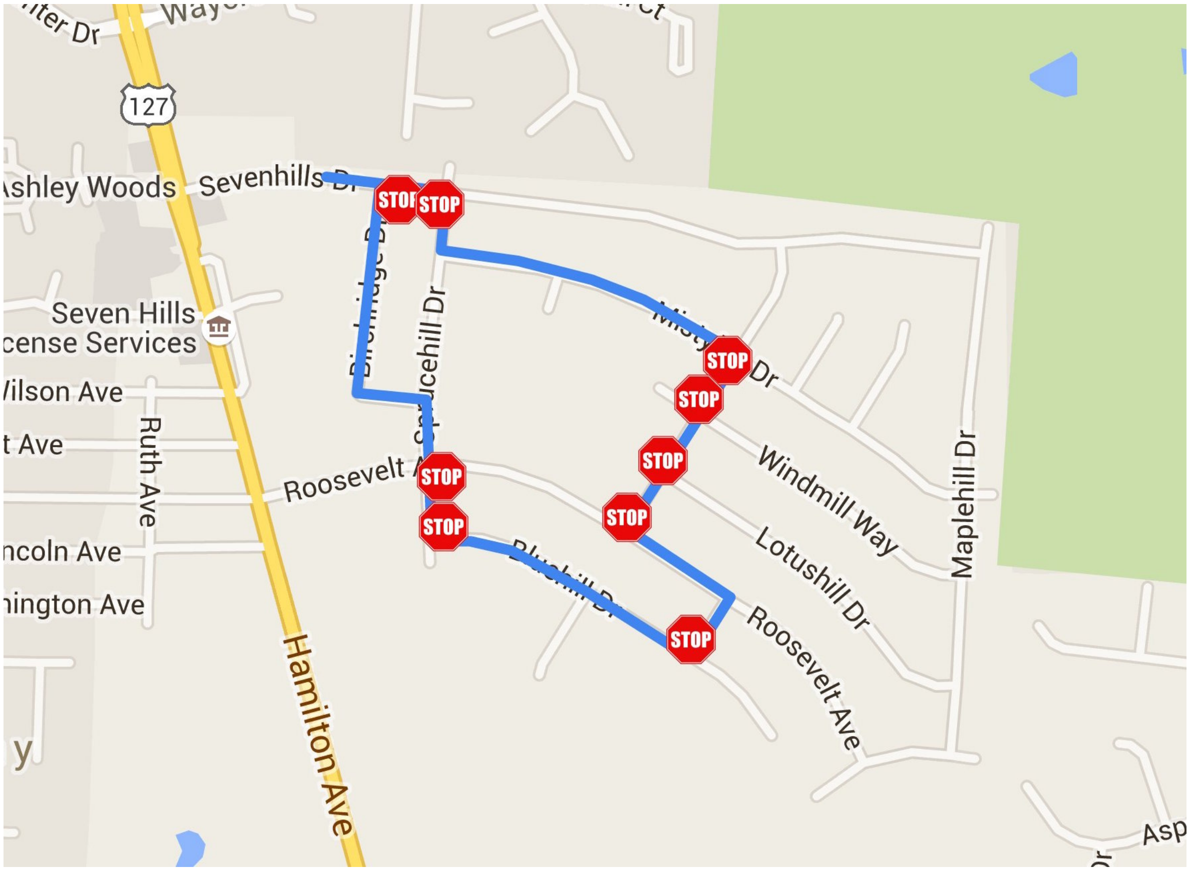

Figure 6.1: Testing Route, 1.4 miles

approximately 80% were legitimate and the remaining 20% had false data (such as not stopping at a legitimate stop sign) injected. The samples were collected at various times of the day and across multiple days, to encompass a wide variety of traffic information and road conditions. Similar to [75], this system applied smartphone sensors, such as gyroscope, accelerometer, magnetometer, etc., to determine the vehicular state at any instant of time, and also logged GPS data as trace points 6.2. The approximate coordinates of the Stop Signs were predetermined and supplied to the machine learning engine.

Driving samples were collected using a smartphone, which was running a custom applica-

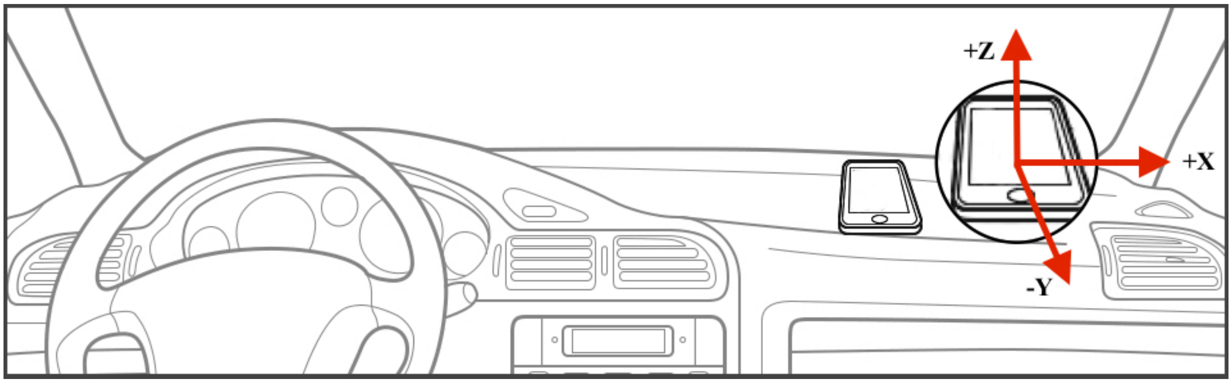

Figure 6.2: Smartphone Placed on the Vehicle's Dashboard Which Acts as a Data Logger

tion. At any instant, the application was recording information such as GPS coordinates, information from the accelerometer, gyroscope and the magnetometer. Given the collected dataset of GPS coordinates, 80% of the same was used for training the classifier while the remaining subset (20%) was used to test it.

6.2 Threat Model

Under this case, we consider a threat model wherein the adversary has the capability of physically compromising a self-driving car by hoodwinking it. In this model, an adversary is a person waiting to cause physical damage to the vehicle (carjacking) by providing false visual information to the vehicle (false regulatory sign). Malicious entry is yet still possible by providing misleading information to vehicles, causing them to be rerouted onto unsafe trajectories. This is an overall simplistic threat model where all the attacker has to do is to place (or remove) a road sign, which can lead to malicious consequences of various degrees.

Scenarios

The goal is to understand the potential implications of providing falsified information to intelligent vehicles and how the same may benefit a potential adversary. While most of this work relates to the theory of the system which recognizes suspicious events, we also explore potential scenarios where the proposed system may find application.

- Suppose Alice is "driving" her intelligent vehicle along an unfamiliar road at night (or an isolated one), a Stop Sign comes up and the vehicle recognizes it as it becomes visible. What the vehicle is unaware of is that the sign was intentionally placed by an adversary, with the intention of physically overpowering the vehicle. As is the expected behaviour, the vehicle slows down and makes the necessary stop at the sign, when suddenly someone (one or more) attacks the car and forces entry into the vehicle in that moment.
- Suppose Bob is "driving" his intelligent vehicle along circumstances similar to the previous case when a sign comes up asking the vehicle to take a detour. Similar to earlier discussion, the sign was intentionally placed by an adversary, with the intention of physically overpowering the vehicle. As is the expected behaviour, the vehicle follows the directions as specified by the sign and finds itself at a dead end (or similar), rendering it a sitting duck.

Although hypothetical, these scenarios project how vehicular compromise can be of varying degrees and how different scenarios need to be considered when designing solutions to address transportation needs.

Extended Use Cases

In addition to what has already been defined, the proposed architecture serves multiples purposes. It may also address some of the deficits of interoperability as created by high definition (HD) maps, when translated by different vendors. The rendering of HD maps by various vendors implies a stark disconnect between the technology and its uniformity across the space. Robust, real-time and low latency are the key requirements of this technology, paving the way for the future of transportation. Typically, HD maps for highly automated driving also have multiple layers, including navigation, localization, and planning. The proposed architecture aims to sit as another stack or layer in the mapping hierarchy, provided as a standardized service similar to route information such as speed.

In addition to security enhancements, the proposed architecture also encourages safe driving. For example, envision a scenario where a stop sign is placed at an intersection (for X number of years) and one day, given new road laws or a change in landscape or traffic flow, it is removed. In this case, everyday commuters who are used to stopping at the intersection might still continue to do so, out of sheer habit, even when the sign is absent. On the same road, when a AV does not see such a sign and given its design, it might continue it's current motion. Thus, chances of a possible collision is high. By defining thresholds against Equation (6.7), various states may be defined for which a vehicle may exist. This possibly includes a

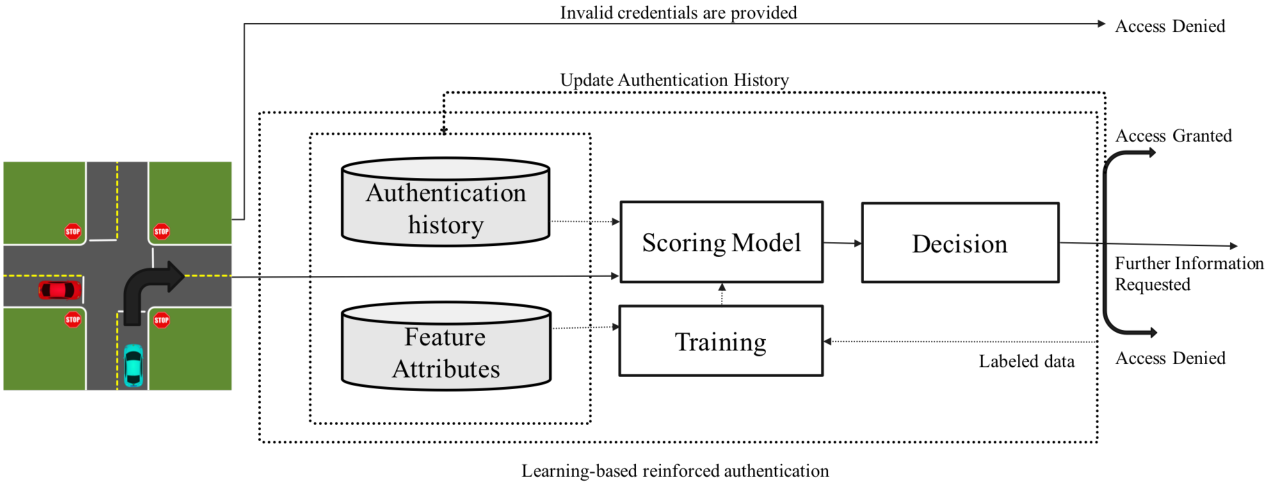
Invalid credentials are provided
Access Denied
Update Authentication History
Access Granted
Authentication history
Scoring Model
Decision
Further Information Requested
Feature Attributes
Training
Labeled data
Access Denied
Learning-based reinforced authentication

Figure 6.3: Architecture of the Proposed System with Learning-Based Reinforced Authentication

stop state, a start state, a continue state or a drive with caution state. This architecture promoted safe driving across the road infrastructure, and supports autonomous vehicles to coexist alongside legacy vehicles (e.g., vehicles with a manual transmission).

6.3 Analysis Methods

The fundamental concept driving this research stems from exploiting complementary information, extending beyond the validation of regulatory signs along the road. The aforementioned information maybe extracted by maintaining a history of all the times vehicles obliged by following the instructions as mandated by the regulatory sign, and then evaluating the feasibility of carrying out those recommended instructions. We take advantage of various context clues, for example a stop sign is more likely to occur near an intersection, so if the computer determines it is not at an intersection, it may be able to rule out a stop sign. Note that the computer has other 'senses' besides sight, for example it has a map, GPS and real-time traffic information.

Assuming $r \in \mathcal{R}$ denotes the coordinates of an observed regulatory sign, with $\mathbf{v} = (v^1, ..., v^x) \in \mathcal{V}$ representing a x-dimensional set of *feature vectors* which typify an observed regulatory sign (e.g. coordinates, intersection specifications, crash reports, traffic volume, etc), and $y \in \mathcal{Y} = \{L, M\}$ symbolizing the class categories of a legitimate fixture (L) or a masquerade attack (M). For the remainder of this chapter, uppercase letters will be applied to describe random variables (r.v.) and lowercase letters stand for the corresponding instantaneous values. Suppose, if r.v. $\mathcal{V}$ represents the coordinates of a regulatory sign, then v is the coordinate at any instance (e.g. $(longitude, latitude)$). It is assumed that for each regulatory sign, samples of either class categories have been rendered as per the specifications of an otherwise unknown underlying probability distribution model $p(\mathbf{V}, \mathcal{R}, \mathcal{Y})$, against which only a limited set of samples $\mathcal{S} = \{v_i, r_i, y_i\}_{i=1}^{n}$ is made available. Here, $\mathcal{S}$ represents an attempt being made towards a *perceptive handshake* for each regulatory sign. In a general communications theory, a handshake refers to the process wherein two devices initiate communication, thereby establishing a communication channel. Here, the term *perceptive handshake* refers to the intuitive communication between a regulatory sign and the corresponding vehicle it is communicating with. Once the vehicle establishes the instructions on the sign, it performs the corresponding suggested actions by establishing a mutual connection between them based on visual cues. Another assumption made is that the credentials being provided to enable *perceptive handshake* are valid, and have not been tampered with. It is assumed that if the credentials are incorrect, then the attempt at *perceptive handshake* shall be denied, irrespective of the output generated by the ground truth module.

Deciphering the ground truth can be modelled as a process of learning a classification function $f : \mathcal{V} \times \mathcal{R} \mapsto \mathcal{Y}$ such that, for every instance of feature vector $\mathbf{v}$ and coordinate r, it can predict whether the attempted *perceptive handshake* is legitimate or not. This function is referred to as $f_r(\mathbf{v}) \in \{L, M\}$.

The Maximum-A-Posteriori (MAP) criterion may be determined by:

$$\arg\max_{y \in \mathcal{Y}} p\big(\mathcal{Y} = y | \mathcal{V} = v, \mathcal{R} = r\big). \tag{6.1}$$

Equation 6.1 represents the decision yielding function such that it determines the minimum probability of a wrong prediction (i.e. it minimizes risk of generalization error). This is computed given the distribution model p is a known statistic. Given the two class distinctions, the MAP criterion ascertains if $\mathcal{Y} = M$ if

$$\frac{p(\mathcal{Y} = M | \mathcal{V} = v, \mathcal{R} = r)}{p(\mathcal{Y} = L | \mathcal{V} = v, \mathcal{R} = r)} > 1, \tag{6.2}$$

and $\mathcal{Y} = L$ for the remaining scenarios. Bayes' Theorem when applied to numerator and denominator of equation (2), it yields

$$\frac{p(\mathcal{Y} = M | \mathcal{V} = v, \mathcal{R} = r)}{p(\mathcal{Y} = L | \mathcal{V} = v, \mathcal{R} = r)} = \frac{p(\mathbf{v}, r | \mathcal{Y} = M)}{p(\mathbf{v}, r | \mathcal{Y} = L)} \frac{p(\mathcal{Y} = M)}{p(\mathcal{Y} = L)}. \tag{6.3}$$

Given that the prior probabilities are independent of v and r, the MAP criterion is updated to

$$\underbrace{\frac{p(\mathbf{v}, r|\mathcal{Y} = M)}{p(\mathbf{v}, r|\mathcal{Y} = L)}}_{h_r(v)} \lessgtr \underbrace{\frac{p(\mathcal{Y} = M)}{p(\mathcal{Y} = L)}}_{\theta}. \tag{6.4}$$

Equation (4) implies that $\mathcal{Y} = M$ if $h_r(\mathbf{v}) > \theta$, and $\mathcal{Y} = L$ in the remaining cases. To accommodate for the trade-off between the rate of misclassified legitimate attempts at *perceptive handshake* (referred to as FP or false positives) and the attack detection rate (referred to as TP or true positives), the threshold θ may be adjusted against a validation set. This rule is also more popularly known as *likelihood ratio* or the *Neymann-Pearson criterion*. The Neymann-Pearson lemma states that for a given FP rate, θ is selected such that the likelihood ratio test maximizes TP (detection rate). When the probability distributions $p(M|\mathbf{v}, r)$ and $p(L|\mathbf{v}, r)$ are known in advance, the rules performs in the optimal circumstances by yielding the maximum detection rate. However, in practical circumstances, the probability distributions are an unknown quantity, and they are in fact estimated from the available data-set $\mathcal{S}$. Thus, the accuracy of the likelihood ratio test is proportional to the performance of the distribution estimations.

In the event that the confidence score $h_r(v)$ is close to the value of θ (the estimated threshold), this implies that the prediction is not very confident, then additional logistical information (such as information about the other vehicles on the road, and what they are sensing) may be prompted for, to validate the authenticity of the road fixture. For such cases, there is a need for two types of thresholds to be defined and applied, such that $\theta^r > \theta^x$:

$$f_r(v) = \begin{cases} M, & \text{if } h_r(v) > \theta^r, \\ P, & \text{if } \theta^x \leq h_r(v) \leq \theta^r, and \\ L, & \text{if } h_r(v) < \theta^x, \end{cases} \tag{6.5}$$

where P represents the cases wherein extra information is promoted or requested. This case is typically referred to as classification with a reject option.

Assumptions

Given $p(v, r|y) = p(v|r, y)p(r|y)$, equation (4) can be represented as:

$$h_r(v) = \frac{p(\mathbf{v}|r, M)}{p(\mathbf{v}|r, L)} \frac{p(r|M)}{p(r|L)} \tag{6.6}$$

A limitation of this system is that data is sparse, which implies that little information is available for training each class distinction. For example, given hysteresis and approximation errors associated with GPS data, getting exact pairings between the coordinates of the regulatory sign and the road topology is a problem, thus estimating $p(\mathbf{v}|r, y)$ for either class is a challenge. To account for this inherent shortcoming, it is assumed that the participating feature vectors are independent of each other, i.e. $p(\mathbf{v}) = \prod_{k=1}^{x} p(v^k)$. In the realm of text categorization and spam filtering, this is a well established technique for estimating multivariate probability distributions. Also, it is assumed that in the event of an attack, the specific coordinate r logged is independent of the feature vector set $\mathbf{v}$ as used by the attacker, i.e. $p(v|r, M) = p(v|M)$. This is beneficial as it accounts for *indiscriminate attacks*, that is attacks are aimed at compromising the integrity of the system rather that one isolated case. This is because it is assumed that the attacker is incapable of deciphering the value of v as logged by previous events such that the values of (v, r) maybe adjusted accordingly.

Thus, $p(v|r, M) = \prod_{k=1}^{x} p(v^k|M)$ and $p(v|r, L) = \prod_{k=1}^{x} p(v^k|L)$. Additionally, by applying Bayes' Theorem, $p(v^k|M) = p(M|v^k)p(v^k)/p(M)$, substitutions might be made. The term $p(v^k|M)$ may be estimated as a feature reputation system, as further elaborated upon later. By adjusting the value of the decision threshold θ, the terms dependent on $p(M)$ may be disregarded. This yields:

$$h_r(v) = \left(\prod_{k=1}^{x} p(M|v^k) \frac{p(v^k)}{p(v^k|r, L)} \right) \frac{p(r|M)}{p(r|L)} \tag{6.7}$$

Scoring Function

$h_r(v)$ as computed by equation 6.7 serves similar to a scoring function, when in reality it is a probability estimation function. This section explains all the terms that cumulatively estimate the value of $h_r(v)$.

$p(M|v^k)$: Theoretically, the probability for every feature estimate v^k may be estimated from the training data set. However, given that there are insufficient events of an attack being logged for every value of v^k, as an alternative, it is possible to apply a system akin to a *reputation system* to render this factor. Specifications on how such a system might be

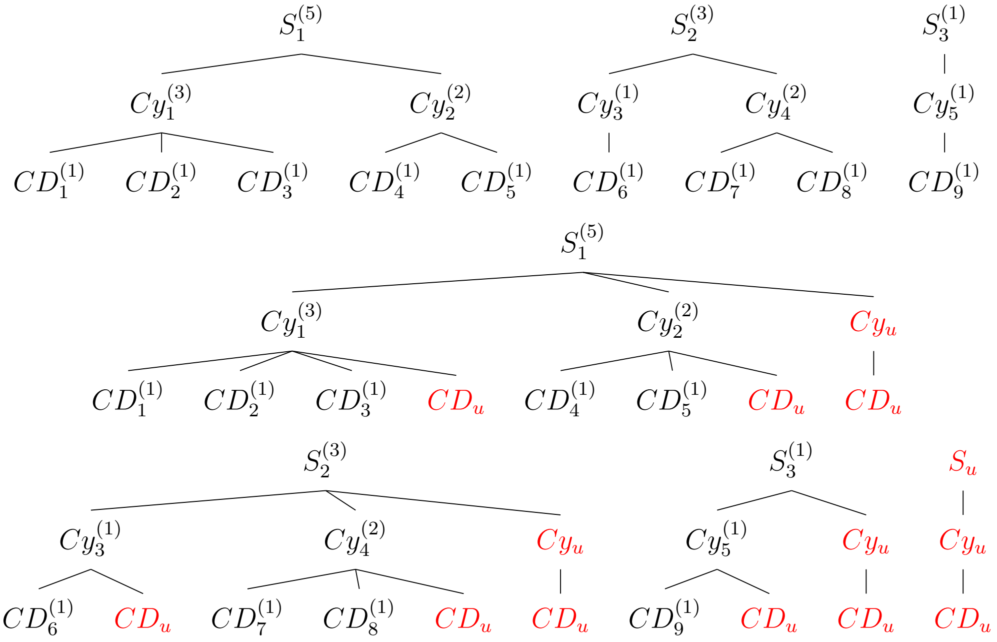

Figure 6.4: An illustration of smoothing probability estimates for unobserved coordinates. The sample set assumes that all the data points belong to a single country, thus the highest level of granularity available is at the state level. Thus the sample set involves 3 States (S), 5 Cities (Cy) and 9 known Coordinates (CD). Unseen events are represented in red. The estimated counts $e(.)$ for each event is denoted using parentheses; e.g., $S_1^{(2)}$ denotes that S_1 has been seen twice. It is assumed that one unseen CD exists per known Cy, unknown Cy and known S, unknown S and known Co, both unknown S and Cy and the case where all Cy, S and Co are unknown. Thus, $U = 5 + 3 + 1 = 9$ of unseen CDs (denoted by CD_u). Applying Eq(8), $S = U = 9$, $p_o(v) = \frac{1}{18}$. When $(k = 1)$, a previously unseen CD originating from S_1 has $p_1(v) = \frac{1}{8} \times \frac{5}{9}$ (the first term represents the smoothed estimate $p(v|z_k)$, including unseen events). If the same CD originates from S_3, then $p_1(v) = \frac{1}{3} \times \frac{1}{9}$. For $(k = 2)$, if the unseen CD originates from Cy_1, then $p_2(v) = \frac{1}{4} \times \frac{3}{9}$. It is to be noted that $p_2(v) > p_1(v) > p_0(v)$. In the event that both S and Cy are unseen, then $p_0(v) = \frac{1}{18}$ and $p_1 = p_2 = 0$.

built is highlighted upon later. A coordinate reputation system will be tasked with having to assign each observed regulatory sign a "reputation score", which is indicative of how likely is the observed regulatory sign been placed with malicious intent. After being normalized, the reputation score may be applied to compute an appropriate probability estimate.

$p(r|M)$: This represents the probability of an attack having occurred for coordinate r. Given, determining the event of a hack may be challenging to determine, it is assumed that all observed regulatory signs have equal likelihood of being masqueraded. A more mature technique may consist of identifying areas or zones which are more prone to come under attack, such as isolated lanes or rarely used road systems.

$p(r|L)$: This is an estimate of the probability that an attempted *perceptive handshake* is legitimate, with the coordinate r being valid.

$p(v^k), p(v^k|r, L)$: This is a historical estimate of the number of times the value of v^k has been reported as a feature of $\mathcal{V}^k$, and can be applied across multiple instances.

As a part of our design model, if new roadblocks or regulatory signs are placed, the system is capable of accounting for the same. This is possible as no single event of compromise is labelled and applied in the computation of $h_r(v)$.

Smoothing

Sparsity of data is a known problem with this infrastructure, with the likelihood of observing a previously unseen value v against $\mathcal{V}$ is plausible. For example, an upcoming construction or an on-going roadwork requires new regulatory signs to be in place. This would imply that v is an unobserved value in the entire global history or even for r. As a result of this, the Maximum Likelihood Estimation (MLE) of $p(v|r, L)$ and $p(v)$ will be zero, rendering equation (7) to be undefined. *Smoothing* is a commonly applied technique to solve this limitation. It has originally been proposed to perform probability estimations for n-gram language models and overcome the adverse affects created by the sparse data.

The concept of smoothing is based on distributing probability estimates between known and unknown events. The probability of mass of known events is decreased to assign some probability estimates which will account for unknown events. Thus, the estimates are adjusted to:

$$p_0(v) = \begin{cases} \frac{e(v)}{S}\Bigg(1 - \frac{U}{S+U}), & \text{if } e(v) > 0, and \\ \\ \frac{1}{S+U}, & \text{otherwise.} \end{cases} \tag{6.8}$$

Here, $e(v)$ refers to the count of the events where v was observed and $S = \sum_v e(v)$ is the total number of events recorded. U unseen events are accounted for by minimizing the estimate $e(v)/S$ by assigning each unseen event a probability mass $1/(S + U)$. For example, suppose $S = 4$ as reported by different vehicles, and $U = 2$ is assumed. The *smoothed* probability $p_0(v)$ of an unknown regulatory sign being observed will be $1/2$, which is the same probability by which a known coordinate would be estimated against (rather than 0 for unseen events).

Applying aggregation to the observed coordinates enables the design of a more efficient scheme for allocation probabilities to different events. Here, we propose that coordinates of observed points be clustered or grouped together based on known topological metrics such as city, state and country. Higher probabilities be allocated to the previously unobserved coordinates which are characterised by known topological vectors. Thus, the estimation of (v) may be updated to:

$$p_k(v) = \sum_{z'_k \in \mathcal{Z}_k} p(v|z'_k)p(z'_k) = p(v|z_k)p(z_k), \tag{6.9}$$

where z'_k represents a conditioning event, assuming values from $\mathcal{Z}_k$. k refers to the granularity of the observed value, with a higher value of k denoting a higher level. For example, $k = 1$ may correspond to countries, $k = 2$ to states and $k = 3$ to cities. $k = 0$ is the default level, denoting all the attempts being made towards a *perceptive handshake*, thus providing a *top view* of the entire communication exchanges. Additionally, a new level ℓ represents the coordinate level, thus implying $z_\ell = v$. In the event that v belong to a different city (or state/country), the probability of observing v belonging to a different city (or state/country) z'_k is zero, thus marginalization in (6.9) results in $p_k(v) = p(v|z_k)p(z_k)$.

By establishing that $p(v|z_k)$ is analogous to equation (6.8), smoothing can be applied to $p(v|z_k)$ by replacing S by S_{z_k} and M by M_{z_k}. The MLE of $p(z_k)$ remains unchanged, resulting in the estimate yielding zero[1]. As such, higher probabilities are allocated to unseen coordinates which originate from known cities/states/countries (refer to Figure 6.4).

[1] When smoothing is not applied, estimates of $p_k(v)$ is same as the ML estimate for $p(v)$

To maintain consistency across the levels, such that $0 < k < \ell$:

$$U_{z_k} = \sum_{z_{k+1} \in z_k} U_{z_{k+1}} + \mu_{z_k}.$$

Here, μ_{z_k} refers to the count of unseen events of coordinates which do not belong to z_k. To initialize the base case, $U_{z_\ell} = 0$ is defined for all coordinates z_ℓ, as no unseen coordinate belongs to a coordinate. $\mu_{z_k} = 1$ for any z_k implies that there exists an unobserved coordinate per city, one unobserved city per state, one unobserved state per country and one unseen country. Then, the top view U is given by one more than the number of observed countries.

Thus, applying the arguments mentioned above, the estimates of $p(v)$ for different values of k may be computed, depending on the findings from the conditioning event z_k at a fixed instance k. Inspired by [76], either *interpolation* or *backoff* may be applied to aggregate the different estimates.

Linear Interpolation

One way of aggregating $p_k(v)$ is by linearly combining them as:

$$p_{linear}(v) = \sum_{k=0}^{\ell} \lambda_k p_k(v). \tag{6.10}$$

The coefficients $\{\lambda_k\}_{k=0}^{\ell}$ is learned by maximising the likelihood estimation over the unobserved data, given the constraint that $\sum_(k = 0)^\ell \lambda_k = 1$. Similar techniques may be applied to estimate $p(v|r, L)$ by limiting the counts to the conditioning cases.

Backoff

Backoff is based on the idea that in the event an observed coordinate has no prior association to a city, "back off" is applied by using data from the city to which the coordinate belongs to. In the event that there are no observations for that city, "back off" is applied to the state, and so on. Thus, $\ell + 1$ probability estimates $p_k(v)$ for $k = 0, ..., \ell$ is given by:

$$\ddot{p}(v) = \begin{cases} \alpha_l p_l(v), & \text{if } e(z_\ell) > 0, \\ \alpha_{l-1} p_{l-1}(v), & \text{if } e(z_{\ell-1}) > 0, \\ ... \\ \alpha_0 p_0(v), & \mathit{otherwise}. \end{cases} \tag{6.11}$$

As granularity is directly proportional to k, Equation 6.11 implies that the estimates should be computed for the most granular level at which the data exists. $\sum_v \ddot{p}(v) = 1$ is maintained by means of the normalization factors, expressed by the coefficients $\alpha_0, ..., \alpha_\ell$.

As mentioned previously, $p_k(v) = p(v|z_k)p(z_k)$, where $p(v|z_k)$ refers to the *smoothed* estimate of observing the coordinate v in the entity z_k, and $p(z_k)$ is the *unsmoothed* estimate of observing the entity z_k. The value of $\ddot{p}(v)$ in equation 6.10 denotes how the chosen granularity affects the overall performance of the estimates. If v is selected from a known estimate (unsmoothed), then $p_l(v) = p(z_l) = e(v)/S$ whereas for a smoothed estimate $\ddot{p}(v) = p(v|world) = e(v)/(S + U)$.

Feature Weighting

Equation 6.7 yielded a scoring function $h_r(v)$, wherein all the features are assigned an equal weight. In event that a compromise occurs and labelled data is present, certain features may prove to be more sensitive than others. Thus, to incorporate this property, the scoring function can be updated to:

$$\hat{h}_r(v) = \left(\prod_{k=1}^{x} p(M|v^k)^{\alpha_k} \frac{p(v^k)^{\beta_k}}{p(v^k|r, L)^{\gamma_k}} \right) \frac{p(r|M)^{\delta}}{p(r|L)^{\epsilon}}, \tag{6.12}$$

where $\alpha_k, \beta_k, \gamma_k, \delta$ and ϵ are real-valued weights. The value of the weights can be determined by learning from the labelled data set by means of a logistic regression classifier, specifically, against $\log(\hat{h}_r(v))$.

6.4 Reputation System

The goal of this scoring model is to provide a holistic view of the legitimacy of the observed features; developed and designed to be scalable and real-time. The first step in the pipeline is to group the observed coordinate(s) for the roadside fixture into clusters, where the coordinates and topological information serve as *cluster-level* features, which are then fed into a machine learning engine. Following the clustering process, a training model is defined with the aim of presenting good predictors for classification purpose.

Clustering Geo-locations

As the name implies, the cluster builder takes the raw data and builds clusters based on provided features. K-means is a relatively popular clustering technique and extremely appealing from a statistical and signal processing point of view as it is designed to minimize variance. However, it does not meet the brief in this scenario as the data is non-linear in nature. Traditional clustering techniques require the use of geodetic distance functions to determine the precision of the decision model. It is imperative for a good classifier to be able to account for *arbitrary* distance functions. Some of the more popular methodologies for performing geospatial clustering are hierarchical clustering [77], PAM [78], CLARA [79], and DBSCAN [80].

Post-clustering is important to profile each cluster to determine its accuracy and consistency. It is advisable for each cluster to maintain basic statistical uniformity, which includes computing means or quartiles for the collected data. It is also necessary to design a temporal system as large gaps in time between readings could cause incorrect data to be logged. Thus, computing frequency and mapping frequency determine the nature of the distribution and is another additional benefit.

Support Vector Machine

A support vector machine (SVM) is a learning algorithm which describes a decision function as a solution of an optimal hyperplane, which is defined in a high dimensional space

[81], [82].

The training dataset consists of pairs $\{(s^{(i)}, t^{(i)})\}_{i=1}^{m} \in \Re^n \times \{0, 1\}$. Here, m is the number of training samples, $s^{(i)}$ is the set of feature inputs and $y(i) \in \{0, 1\}$, with $\Re$ representing the model parameters. SVM with a radial basis function (RBF) kernel is adopted, rendering the SVM as a non-linear classifier. The RBF may be formulated as $k(s, s') = \exp(-r||s - s'||^2)$, where r refers to the *kernel bandwidth* and is dependent upon the results of cross-validation.

Theoretically, the SVM classifier begins by mapping s to a higher dimensional space as a function ϕ, following which it searches for a hyperplane H with the aim of maximizing the distance between $\phi(s_i)$ and H. If $< \omega, S >= b$ represents the hyperplane and S exists in the higher-dimensional space, then $f(s) =< \omega, \phi(s) > -t$ represents the decision function. The class labels of s are determined by the sign of f. We recommend adopting a probability model for classification purposes. This can be done by fitting the decision estimates for the binary classifiers to a logistic distribution by means of a maximum likelihood. This enables the output to be a numerical score, indicating probabilities. By mapping the scores to a probability estimates allows for it to find place in equation 6.7.

To evaluate the effectiveness of the model, the same training and validation set is used. However, $p(M|v)$, that is the reputation score for all the feature values of v is set to be identical.

Table 6.1: Cluster level: 80-20 split testing performance

Algorithm	**Area under the Curve**	**Recall@p95**
SVM	0.986	0.947

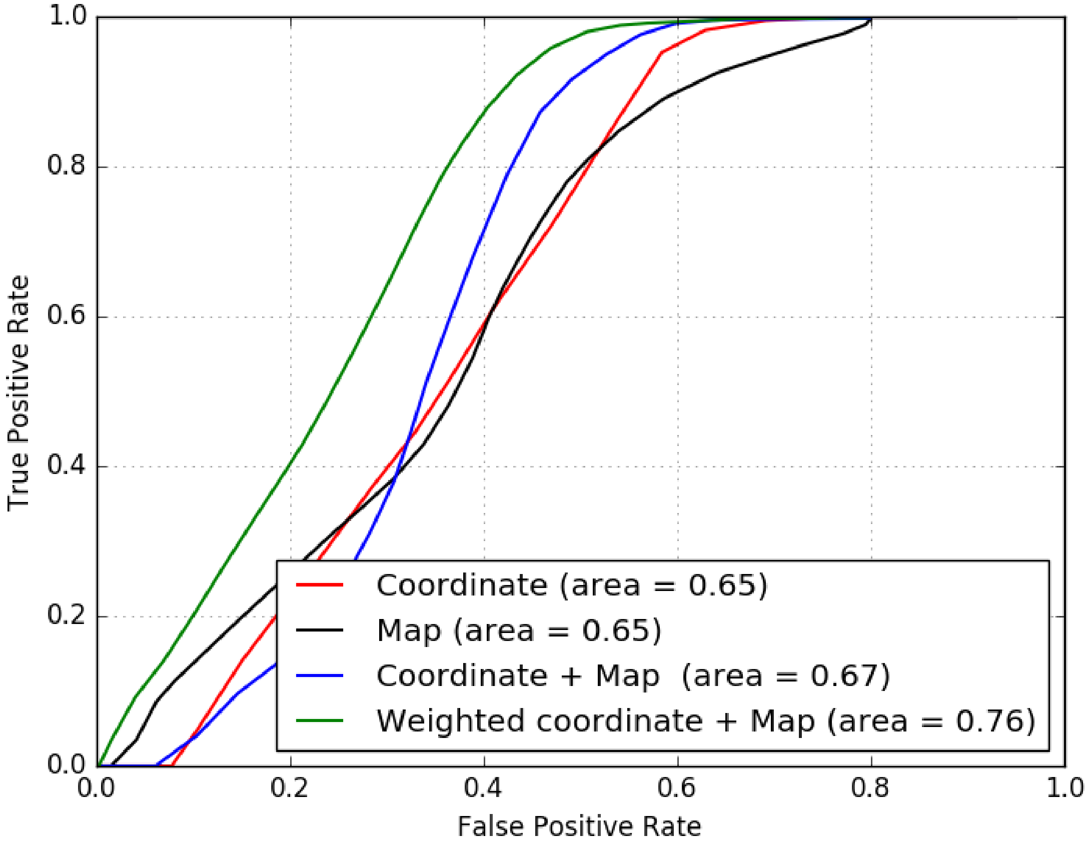

Figure 6.5: Backoff Smoothing

As a part of the cluster builder module stated earlier, support vector machine was used to generate cluster labels using three distinct thresholds. The defined thresholds are 20%, 65% and 80%, and the corresponding Area under the Curves are 0.985, 0.987 and 0.988, respectively. This suggests that the relative ordering of scoring is independent of the selected threshold. Following this, SVM is applied to evaluate the performance of the scoring model. The parameters of the supervised learning algorithms are established by applying an $80-20$ split cross-validation process. This implies that 80% of the sample data set was used as training

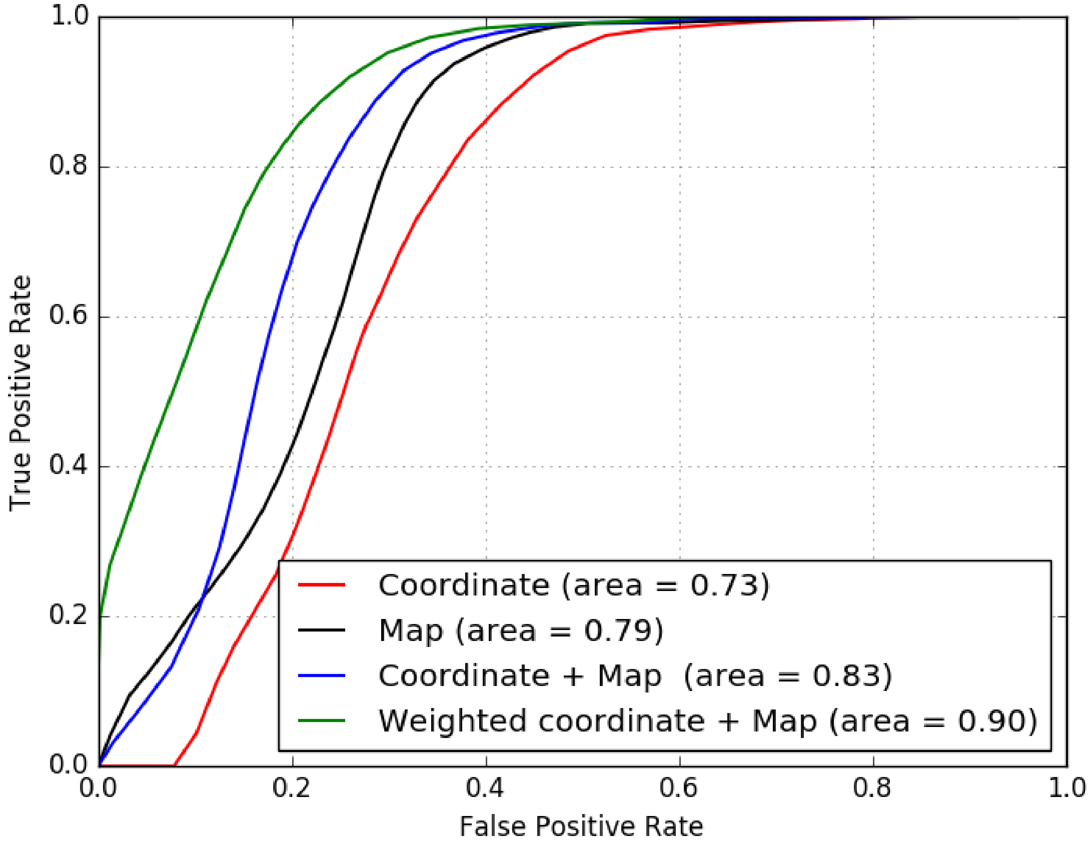

Figure 6.6: Interpolation Smoothing

samples while the remaining 20% is used for purposes of performance testing. Table 6.1 represents the in-sample performance at the cluster level as measured by Area under the Curve and when the recall was set at 95% precision.

Table 6.2: Vehicular level: 80-20 split testing performance

Algorithm	**Area under the Curve**	**Recall@p95**
SVM	0.978	0.900

Vehicular level implies that every attempted event of *perceptive handshake* is assigned

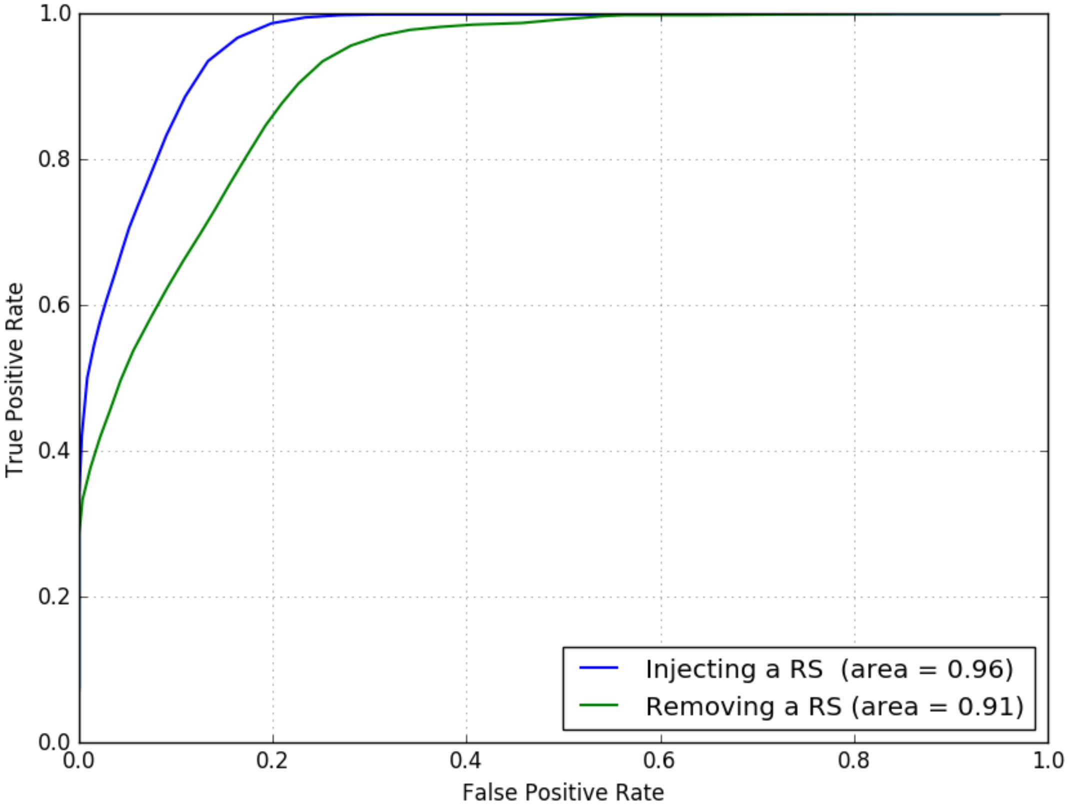

Figure 6.7: Evasion Attacks

the score computed at the cluster level for those observed coordinates. Table 6.2 is a representation of the testing Area under the Curve and recall (at 95% precision) at the vehicular level. This is driven by the performance of the clustering algorithm, which in turn improves the performance of the classifiers. In addition to the scenarios already accounted for, out-of-sample data is also evaluated to test the execution of the model. The use-case for doing so is to take into account events where data failed to be reported or given poor visibility conditions, trace points were not available, causing failure. Thus, to emulate close-to-reality scenarios, out-of-sample analysis is performed (Fig 6.8).

Table 6.3: Cluster level: Out-of-sample testing performance

Algorithm	**Area under the Curve**	**Recall@p95**
SVM	0.968	0.759

Table 6.4: Vehicular level: Out-of-sample testing performance

Algorithm	**Area under the Curve**	**Recall@p95**
SVM	0.952	0.714

The out-of-samples performance evaluation is represented in Tables 6.3 and 6.4, for cluster and vehicular level respectively. The results indicated that there is a need to retrain the model periodically based on incoming data as to account for newer patterns and to increase the probability of determining fake events. Additionally, as noted from the results obtained, it may be noted that the performance of the SVM classifier decreases from the cluster level to the vehicular level. This implies that SVM performs better at classifying small clusters, thereby providing a performance boost.

To evaluate the performance of our proposed model, simulated data set attacks were performed wherein using random sampling, two distinct kinds of attacks were performed on the data set. In one case, it is assumed that a known RS is removed from the road network and in the other scenario, a new RS is introduced into the road network.

Both backoff and interpolation smoothing are evaluated for $\mu_{z_k} = 1$, for all z_k. 50% of the data set was utilized for training, while the remaining 50% is applied for evaluating the performance of the model. Four different feature combinations are used for evaluation

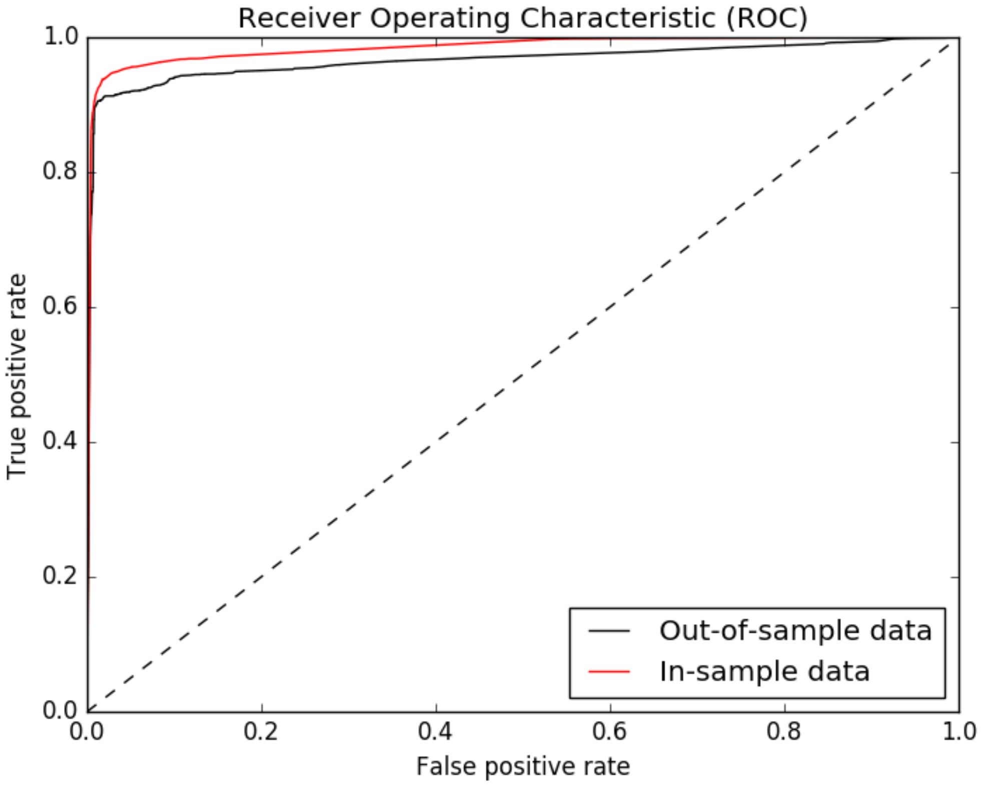

Figure 6.8: ROC Curves for SVM on In-Sample and Out-Sample Data

purposes, using Equation 6.7. The level of granularity assumed is $\ell = 1$, representing the user experience at a native level. Figure 6.5 and 6.6 depicts the ROC curves for the 4 feature combinations. The results depict that both smoothing techniques show similar performance, with interpolation exhibiting slightly better than backoff.

Two types of attacks are simulated, and the model is subjected to the same, with the end of goal of evaluating the strength of the model (Figure 6.7). In the event wherein a fake RS is injected into the road trajectory, an AUC of 0.96 is observed, indicating the model performs well at identifying this type of anomalous behavior. At 10% FPR, almost 96% masquerading attacks could be identified. In the second kind of attack, yielded an AUC of 0.91 and 75% TPR at 10% FPR. The latter proves to be a more challenging attack to circumvent.

6.5 Conclusion and Future Work

This work introduces a framework aimed at questioning and classifying *perceptive handshaking* events into genuine and suspicious activity, based on the parameters provided at communication time. We encourage other researchers to consider more scenarios along these lines. In addition to providing a statistical framework for classification purposes, we have also proposed a machine learning pipeline with the goal of building a reputation system for high definition (or precision) maps. A key design motivation that formed a core force driving the specifications of this model is its ability to adhere to interoperability. This approach is suitable for a wide and diverse user base, for it can be deployed independent of the other vehicles on the road.

This work can be extended in several directions, all of which seem equally promising. While temporal information is applied for building the reputation system, it does not find place in the classification system in its current layout. As a future implementation, temporal correlation can be applied as part of the classifier vector definition. If an event of compromise is marked, then it is highly likely that another compromise will reoccur around the same window, assuming a sufficient number of features match up between both (or more) cases.

For purposes of prototyping, the evaluation of the model presented has been done offline.

That implies that this study consisted of historical data, which is a natural bias given the dynamic nature of road networks. Thus, to truly represent a vehicular network and to find practical application, it would be ideal for this system to perform *real-time* analysis and reporting.

Chapter 7

Summary and Future Work

7.1 Summary

Our future world will consist of a wide array of pervasive devices servicing different needs and applications. These devices will constantly log data of various kinds; including personal, physiological, environmental, etc. This brings us to the problem of ensuring trust and privacy in such systems. With this dissertation, we described four security techniques aimed at providing privacy protocols geared towards three different subsystems in the IoT framework. The sections below highlight upon the contributions we made and what future work maybe pursued with this regards.

Determining alternative biometric parameters for key encryption in WBAN

With the advent of wearable devices and commonality of on-body monitoring devices, it is anticipated that a day will come where body-area networks will become common place in our lives. It is envisioned that the whole process will be automated wherein a user wearing such a device automatically enables the associated security mechanism and establishes communication between that user and her surroundings.This research addresses a technique to identify the wearer of the device and proposes an encryption scheme for secure communication, allowing for identification and authentication before establishing communication. It suggests using gait as a metric for identity association using wearable sensors. For the initial functionality and accuracy testing, a publicly available dataset has been used to determine a unique biometric to be applied for authentication purposes, which we have coined as stride interval. Having established a consistent performance for stride interval, the next step would be to apply the proposed biometric to generate a key to encrypt communication, whose functionality would be similar to that of a session key in a traditional wired network. A known limitation of applying gait as the only biometric is its variance in values due to changes in stance and scenarios. As such, a more accurate dataset would be to collect data from humans in actual working environment rather than simulated settings. As part of the future research, we would analyze real-time data collected from users in transit, under various scenarios and settings, in the hopes of applying machine learning concepts to classify and categorize our findings. To aid in the proper instance matching of humans, we propose to apply multiple sensors to monitor gait. This could also find application in building a hybrid key system to serve as the authentication media. We aim to apply vector concepts for the key generation schemes to design the hybrid encryption key. The overall architecture would work to provide biometric solutions as a viable option for establishing secure communication in a dynamic network environment. It seeks to protect human physiological data in transit, while minimizing energy costs and providing comparably strong security mechanisms. In this research, we have proposed our own key generation scheme. Additionally, as part of this research we look at alternative human monitoring approaches, primarily concentrated around gait. We hope to address the issue of providing identification and consequent authentication using a readily available parameter, thereby providing the technology to recognise individuals in a large subspace. We hope to tackle the problem of recognizing legitimate users from fake ones, thereby subverting privacy issues in WBAN.

Key Management Strategies for WBAN

The purpose of our research is to provide a key management scheme for WBAN and an architecture which would address node compromise and provide network re-traceability. This research is based on the basic probabilistic key distribution techniques that are available to WSN and how they perform for a WBAN. Having established an optimal key distribution scheme, these schemes allow information generated from sensors to be encrypted and decrypted at the coordinator alone. This means that within the communication of the body area network components, all data is hidden and locked from third party listeners. These schemes prevent Man in the Middle attacks from occurring, and also makes provisions for identifying compromised nodes. To determine an optimal key distribution scheme for a WBAN, a 3-Dimensional human movement model was designed and implemented. Humans have 244 possible degrees of freedom, that allows for a varied set of activities and motions to be implemented. However, from a concept perspective, it is difficult to simulate every instance of human motion, as we considered only the most typical movements. Those which have maximum chances of affecting the network topology, causing links to break and reform constantly. Some of these movements included those of a person walking, the hands moving, a synchronized hand and leg posture, etc. We implemented the key distribution schemes along with the movements to determine network connectivity at an instant. Inspired from Merkle Trees and Multivariate Polynomials, these schemes allow public keys to be distributed in the sensor devices from the onset. To determine the performance of our architecture, we built a framework to analyze the performance of our two schemes. We present an analysis of key management schemes in a resource-constrained WBAN. We aim to analyze the changes that can be brought by altering the parameters of a dynamically changing network topology with a limited sensing range. This work provides an end-to-end security scheme for information, with data originating at the sensor based device and terminating at the coordinator. Our scheme has been designed to function in a network which has a pre-defined maximum hop count of 2. We aim to apply this restriction in the network to our advantage and hope to provide an efficient key management scheme for a computationally constrained WBAN.

Reputation system for vehicular mapping and localization

We have proposed a novel architecture aimed at providing secure vehicular mapping mechanisms to compliment and aid autonomous driving systems. This method finds application by sitting upon existing technology stack which is geared towards serving the mapping needs of such systems. The goal is to thwart attempts at carjacking and build an overall system which functions independent of vehicle and requires minimum infrastructural costs.

We have proposed building a reputation system for road-side fixtures based on multiple parameters including and not limited to image recognition systems to identify the road sign, mapping information to determine if the observed road sign is legitimate, real-time traffic information from the high precision map, previously captured historical information, the overall safety score of the area of the present location of the vehicle, etc. This system is designed such that it could accommodate sparse information or be integrated with existing mature infrastructure. By applying a combination of crowd-sourced information and real-time feedback, this system provides multiple safety applications, ranging from threat mitigation to crash avoidance. It provides cautionary feedback to the vehicle, and promotes the idea of having autonomous vehicles coexist with their more legacy counterparts.

To evaluate the proposed system we collected driving information from a fixed route in the city of Cincinnati, and used the same to train and test our machine learning engine. For prototyping purposes the processing was done offline; in the future we imagine this service to exist as a real time cloud based feature.

7.2 Future Work

While there are multiple avenues to pursue research from this point onwards, security research in IoT is no where close to being exhaustive. The open wireless space is plagued with open problems and not enough research or solutions being brought to the forefront. An extension to this work is certainly possible, as have already addressed in each chapter by itself. In addition to what has already been mentioned, we would like to bring to light some other interesting problems which might be pursued. The open research topics being highlighted are merely foundational in nature, and further investigation into each domain might bring to light even greater problems that need necessary addressing.

Fingerprinting Energy Consumption for determining vulnerabilities in WPAN

Recently, researchers have shown that it is possible to compromise devices by tapping into the powerlines. This could include determining users activity using powerline monitoring techniques [83] or reverse engineering home automation devices and using the same to turn against the user [84]. With this research, we propose to apply out of band, physical layer based techniques to determine and detect small anomalies in power patterns with the goal of capturing zero-day attacks. The idea is to design zero-day warning systems for IoT systems. By applying continuous monitoring techniques at minimal installation costs, we can aim to design security solutions which could compliment existing solutions.

On-demand secure connectivity in WPAN

For this research we will be providing security support at the highest level on connectivity available in WBAN, the interaction with the WPAN (Wireless Personal Area Network). A WPAN can be defined as a network for interconnecting devices centered around an individual person's workspace, where the connections are wireless. A typical limitation to the WBAN solutions in present literature works under the assumption that the subject is familiar with his/her environment and most solutions make use of a TA for key sharing purposes. However, with this research we aim to provide an infrastructural support whereby a user can walk into an unknown environment (where his/her network is not already enrolled into the system) and still establish secure communication. With this research, we aim to provide a public key infrastructural support without the need for a TA. In this research, we will be adopting results generated from our previous undertakings and apply that to design a communication architecture towards generating a secure communication channel between devices and their corresponding hosts. This scheme is adapted from the Dynamic Destination-Sequenced Distance Vector Routing (DDSDV) which is a table driven routing scheme for ad-hoc networks. DDSDV is based on the Bellman-Ford algorithm. Similar to the aforementioned routing scheme, we propose to apply key tables instead of the original route table. This research will address network issues such as the compromise of WPAN devices and/or imitation attacks. For determining its efficiency, before commenting on its feasibility, we will be looking at factors such as scalability, overhead, latency and strength. This research is novel in that it would provide on-demand authentication for unregistered devices, and thus provide support for heterogeneous network components. We aim to bring coherency in the entire scheme, with each component working in perfect harmony. There is a possibility of solving what is considered to be a limitation in the public key infrastructure; by overcoming the need for a TA, we are removing another possible weakness in the system, thereby rendering the architecture to be stronger. Data protection and privacy is of the utmost concern and is designed with the same motives.

Applying NTRU to facilitate security in WBAN

In recent times, Elliptic Curve Cryptography (ECC) has emerged as a viable option for public key cryptography in WBAN. ECC allows for comparatively fast computation, small key size and compact signatures. However, ECC is still on the higher side of being computationally complex, rendering it as a less viable solution. We propose to apply a new public key cryptosystem, NTRU to WBAN. Research has shown NTRU as being more secure and faster than ECC, while being computationally less complex. In the scheme of things, a 128 bit ECC provides security comparable to the strength of a 1024 bit RSA key which would be comparable to a 256 bit NTRU key. With this scheme, we aim to provide a new alternative public key cryptosystem based approach to establish security other than more commonly used symmetric systems. NTRU is an open-source public key cryptosystem that applies lattice-based cryptography to encrypt and decrypt data. It also have provisions for designing digital signatures, known as NTRUSign. We can apply NTRU on IEEE 802.15.4 Wireless Body-Area Sensor Networks standard for obtaining secure communication in an indoor environment. We can perform all experimentation's on a TelosB mote platform, running a TinyOS distribution. We will be comparing and evaluating our results from those generated by ECC and Symmetric Encryption. For our purposes, we are concerned with analyzing the latencies, time to authenticate and energy consumption by the NTRU scheme. With this research we will be stating our conclusions on how to combat possible limitations of existing WBAN infrastructure while considering Moore's law. We aim to analyze and state our conclusions on what we deem as an acceptable collateral(s) towards designing a sturdier architecture, including wearable components and network devices. Lastly, we need to consider overhead due to packet transmission and reception that is invoked during the encryption and decryption process. The ultimate goal of this research is to reduce the overall cost of wearable components by extending battery life and performance.

Bibliography

[1] Chun-Wei Tsai, Chin-Feng Lai, Athanasios V. Vasilakos, "Future internet of things: Open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014, ISSN: 1572-8196. DOI: 10.1007/s11276-014-0731-0. [Online]. Available: http://dx.doi.org/10.1007/s11276-014-0731-0.

[2] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, ISSN: 1570-8705. DOI: http://dx.doi.org/10.1016/j.adhoc.2012.02.016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674.

[3] Sara Hachem, Thiago Teixeira and Valérie Issarny, "Ontologies for the internet of things," *Proceedings of the 8th Middleware Doctoral Symposium*, 3:1–3:6, 2011. DOI: 10.1145/2093190.2093193. [Online]. Available: http://doi.acm.org/10.1145/2093190.2093193.

[4] N. Semiconductors, *Smart connected solutions for the internet of things (iot)*, `http://www.nxp.com/applications/solutions-for-the-iot-and-adas/smart-connected-solutions-for-the-iot:SMART-CONNECTED-SOLUTIONS`, 2016.

[5] K. Koscher and A. Czeskis and F. Roesner and S. Patel and T. Kohno and S. Checkoway and D. McCoy and B. Kantor and D. Anderson and H. Shacham and S. Savage, "Experimental security analysis of a modern automobile," *2010 IEEE Symposium on Security and Privacy*, pp. 447–462, May 2010, ISSN: 1081-6011. DOI: `10.1109/SP.2010.34`.

[6] Stefan Poslad, *Ubiquitous computing: Smart devices, environments and interactions*. John Wiley & Sons, 2011.

[7] Mark A Hanson and Harry C Powell Jr and Adam T Barth and Kyle Ringgenberg and Benton H Calhoun and James H Aylor and John Lach, "Body area sensor networks: Challenges and opportunities," *Computer*, vol. 42, no. 1, p. 58, 2009.

[8] Sana Ullah and Henry Higgins and Bart Braem and Benoit Latre and Chris Blondia and Ingrid Moerman and Shahnaz Saleem and Ziaur Rahman and Kyung Sup Kwak, "A comprehensive survey of wireless body area networks," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012, ISSN: 1573-689X. DOI: `10.1007/s10916-010-9571-3`. [Online]. Available: `http://dx.doi.org/10.1007/s10916-010-9571-3`.

[9] Haowen Chan and Adrian Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103–105, Oct. 2003, ISSN: 0018-9162. DOI: `10.1109/MC.2003.1236475`.

[10] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, pp. 41–47, 2002. DOI: `10.1145/586110.586117`. [Online]. Available: `http://doi.acm.org/10.1145/586110.586117`.

[11] Donggang Liu and Peng Ning and Rongfang Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, Feb. 2005, ISSN: 1094-9224. DOI: `10.1145/1053283.1053287`. [Online]. Available: `http://doi.acm.org/10.1145/1053283.1053287`.

[12] Chris Karlof and Naveen Sastry and David Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pp. 162–175, 2004. DOI: `10.1145/1031495.1031515`. [Online]. Available: `http://doi.acm.org/10.1145/1031495.1031515`.

[13] Cynthia Kuo and Mark Luk and Rohit Negi and Adrian Perrig, "Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes," *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*, SenSys '07, pp. 233–

246, 2007. DOI: 10.1145/1322263.1322286. [Online]. Available: http://doi.acm.org/10.1145/1322263.1322286.

[14] Yee Wei Law and Giorgi Moniava and Zheng Gong and Pieter Hartel and Marimuthu Palaniswami, “Kalwen: A new practical and interoperable key management scheme for body sensor networks,” *Security and communication networks*, vol. 4, no. 11, pp. 1309–1329, 2011.

[15] Sarah Irum and Aftab Ali and Farrukh Aslam Khan and Haider Abbas, “A hybrid security mechanism for intra-wban and inter-wban communications,” *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[16] M. Rahman and S. Sampalli, “A hybrid key management protocol for wireless sensor networks,” *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 769–776, Jun. 2012, ISSN: 2324-898X. DOI: 10.1109/TrustCom.2012.32.

[17] W. Louis and D. Hatzinakos and A. Venetsanopoulos, “One dimensional multi-resolution local binary patterns features (1dmrlbp) for regular electrocardiogram (ecg) waveform detection,” *2014 19th International Conference on Digital Signal Processing*, pp. 601–606, Aug. 2014, ISSN: 1546-1874. DOI: 10.1109/ICDSP.2014.6900735.

[18] Charlie Miller and Chris Valasek, “Adventures in automotive networks and control units,” *DEF CON*, vol. 21, pp. 260–264, 2013.

[19] Stephen Checkoway and Damon McCoy and Brian Kantor and Danny Anderson and Hovav Shacham and Stefan Savage and Karl Koscher and Alexei Czeskis and Franziska Roesner and Tadayoshi Kohno and others, "Comprehensive experimental analyses of automotive attack surfaces.," *USENIX Security Symposium*, 2011.

[20] Ruud M Bolle and Jonathan Connell and Sharath Pankanti and Nalini K Ratha and Andrew W Senior, *Guide to biometrics*. Springer Science & Business Media, 2013.

[21] Rajat Kumar Das and Sudipta Mukhopadhyay and Puranjoy Bhattacharya, "User authentication based on keystroke dynamics," *IETE Journal of Research*, vol. 60, no. 3, pp. 229–239, 2014. DOI: `10.1080/03772063.2014.914686`. eprint: `http://dx.doi.org/10.1080/03772063.2014.914686`. [Online]. Available: `http://dx.doi.org/10.1080/03772063.2014.914686`.

[22] Davrondzhon Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," *Annual Norwegian computer science conference*, pp. 19–21, 2007.

[23] Giovanni Alfonso Borelli and Jean Bernoulli and Nikolaus Elinger and Carolus Joannes Jesu, *De motu animalium*. Apud Petrum Gosse, 1743.

[24] Yanmei Chai and Jinchang Ren and Rongchun Zhao and Jingping Jia, "Automatic gait recognition using dynamic variance features," *Automatic Face and Gesture Recognition, 2006. FGR 2006. 7th International Conference on*, pp. 475–480, 2006.

[25] James B Hayfron-Acquah and Mark S Nixon and John N Carter, “Automatic gait recognition by symmetry analysis,” *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2175–2183, 2003.

[26] Girija Chetty and Prasad Yarlagadda and Vamsi Madasu and Anurag Mishra, “Multiview gait biometrics for human identity recognition,” *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, pp. 358–363, 2014.

[27] Flavio Firmani and Stephen N Robinovitch and Edward J Park, “Biometric system for measuring gait and fall characteristics captured on video,” *Journal of biomechanical engineering*, vol. 136, no. 7, p. 071 005, 2014.

[28] Ju Han and Bir Bhanu, “Individual recognition using gait energy image,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 28, no. 2, pp. 316–322, 2006.

[29] Zongyi Liu and Sudeep Sarkar, “Improved gait recognition by gait dynamics normalization,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 28, no. 6, pp. 863–876, 2006.

[30] Jaakko Suutala and Juha Röning, “Towards the adaptive identification of walkers: Automated feature selection of footsteps using distinction-sensitive lvq,” *Proceedings of International Workshop on Processing Sensory Information for Proactive Systems*, pp. 61–67, 2004.

[31] Lee Middleton and Alex A Buss and Alex Bazin and Mark S Nixon, “A floor sensor system for gait recognition,” *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on*, pp. 171–176, 2005.

[32] Heikki J Ailisto and Mikko Lindholm and Jani Mantyjarvi and Elena Vildjiounaite and Satu-Marja Makela, “Identifying people from gait pattern with accelerometers,” *Defense and Security*, pp. 7–14, 2005.

[33] Davrondzhon Gafurov and Einar Snekkenes and Tor Erik Buvarp, “Robustness of biometric gait authentication against impersonation attack,” *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, pp. 479–488, 2006.

[34] Davrondzhon Gafurov and Kirsi Helkala and Torkjel Søndrol, “Gait recognition using acceleration from mems,” *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 6–pp, 2006.

[35] Davrondzhon Gafurov and Einar Snekkenes and Patrick Bours, “Gait authentication and identification using wearable accelerometer sensor,” *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on*, pp. 220–225, 2007.

[36] Yu Zhong and Yunbin Deng, “Sensor orientation invariant mobile gait biometrics,” *Biometrics (IJCB), 2014 IEEE International Joint Conference on*, pp. 1–8, 2014.

[37] Sangil Choi and Ik-Hyun Youn and Richelle LeMay and Scott Burns and Jong-Hoon Youn, “Biometric gait recognition based on wireless acceleration sensor using k-nearest

neighbor classification," *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pp. 1091–1095, 2014.

[38] Gunnar Johansson, "Visual motion perception.," *Scientific American*, 1975.

[39] Shu Nishiguchi and Minoru Yamada and Koutatsu Nagai and Shuhei Mori and Yuu Kajiwara and Takuya Sonoda and Kazuya Yoshimura and Hiroyuki Yoshitomi and Hiromu Ito and Kazuya Okamoto and others, "Reliability and validity of gait analysis by android-based smartphone," *Telemedicine and e-Health*, vol. 18, no. 4, pp. 292–296, 2012.

[40] Jeffrey M Hausdorff and Patrick L Purdon and CK Peng and ZVI Ladin and Jeanne Y Wei and Ary L Goldberger, "Fractal dynamics of human gait: Stability of long-range correlations in stride interval fluctuations," *Journal of Applied Physiology*, vol. 80, no. 5, pp. 1448–1457, 1996.

[41] Saibal K Ghosh and Anagha Jamthe and Suryadip Chakraborty and Dharma P Agrawal, "Secured wireless medical data transmission using modified elliptic curve cryptography," *Proceedings of the 3rd ACM MobiHoc workshop on Pervasive wireless healthcare*, pp. 19–24, 2013.

[42] Frank Louis Carle and Mike R Strub, "A new method for estimating population size from removal data," *Biometrics*, pp. 621–630, 1978.

[43] Black, Paul E, "Fisher-yates shuffle," *Dictionary of Algorithms and Data Structures*, vol. 19, 2005.

[44] Pallavi Meharia and Dharma P. Agrawal, "A hybrid key management scheme for healthcare sensor networks," *2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, May 2016. DOI: `10.1109/ICC.2016.7511484`.

[45] Nils Gura and Arun Patel and Arvinderpal Wander and Hans Eberle and Sheueling Chang Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," in, Springer, 2004, pp. 119–132.

[46] An Liu and Peng Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," *International Conference on Information Processing in Sensor Networks, 2008. IPSN '08.*, pp. 245–256, Apr. 2008. DOI: `10.1109/IPSN.2008.47`.

[47] Nuria Oliver and Fernando Flores-Mangas, "Healthgear: A real-time wearable system for monitoring and analyzing physiological signals," *Wearable and Implantable Body Sensor Networks, International Workshop on*, pp. 61–64, 2006. DOI: `http://doi.ieeecomputersociety.org/10.1109/BSN.2006.27`.

[48] Jason WP Ng and Benny PL Lo and Oliver Wells and Morris Sloman and Nick Peters and Ara Darzi and Chris Toumazou and Guang-Zhong Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (ubimon)," *International Conference on Ubiquitous Computing (Ubicomp)*, 2004.

[49] David Malan and Thaddeus Fulford-Jones and Matt Welsh and Steve Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," *International workshop on wearable and implantable body sensor networks*, vol. 5, 2004.

[50] M. Meingast and T. Roosta and S. Sastry, "Security and privacy issues with health care information technology," *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, pp. 5453–5458, Aug. 2006, ISSN: 1557-170X. DOI: `10.1109/IEMBS.2006.260060`.

[51] F. Kargl and E. Lawrence and M. Fischer and Yen Yang Lim, "Security, privacy and legal issues in pervasive ehealth monitoring systems," *Mobile Business, 2008. ICMB '08. 7th International Conference on*, pp. 296–304, Jul. 2008. DOI: `10.1109/ICMB.2008.31`.

[52] Pallavi Meharia and Dharma P. Agrawal, "The human key: Identification and authentication in wearable devices using gait," *Journal of Information Privacy and Security*, vol. 11, no. 2, pp. 80–96, 2015. DOI: `10.1080/15536548.2015.1046286`. eprint: `http://dx.doi.org/10.1080/15536548.2015.1046286`. [Online]. Available: `http://dx.doi.org/10.1080/15536548.2015.1046286`.

[53] Ming Li and Shucheng Yu and Joshua D. Guttman and Wenjing Lou and Kui Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sen. Netw.*, vol. 9, no. 2, 18:1–18:35, Apr. 2013, ISSN: 1550-4859. DOI: `10.1145/2422966.2422975`. [Online]. Available: `http://doi.acm.org/10.1145/2422966.2422975`.

[54] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM Conference on Computer and Commu-*

nications Security, CCS '02, pp. 41–47, 2002. DOI: 10.1145/586110.586117. [Online]. Available: http://doi.acm.org/10.1145/586110.586117.

[55] Haowen Chan and Adrian Perrig and Dawn Song, "Random key predistribution schemes for sensor networks," *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pp. 197–213, May 2003, ISSN: 1081-6011. DOI: 10.1109/SECPRI.2003.1199337.

[56] WenliangDu and Ronghua Wang and Peng Ning, "An efficient scheme for authenticating public keys in sensor networks," *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pp. 58–67, 2005. DOI: 10.1145/1062689.1062698. [Online]. Available: http://doi.acm.org/10.1145/1062689.1062698.

[57] Lakshmi Santhanam and Bin Xie and Dharma P Agrawal, "Secure and efficient authentication in wireless mesh networks using merkle trees," *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, pp. 966–972, Oct. 2008. DOI: 10.1109/LCN.2008.4664310.

[58] Department of Homeland Security, "Attack surface: Healthcare and public health sector," English, p. 11, 2012. [Online]. Available: http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

[59] Alfred J Menezes and Paul C Van Oorschot and Scott A Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[60] Adrian Perrig and Robert Szewczyk and J. D. Tygar and Victor Wen and David E. Culler, “Spins: Security protocols for sensor networks,” *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002, ISSN: 1022-0038.

[61] Sencun Zhu and Sanjeev Setia and Sushil Jajodia, “Leap+: Efficient security mechanisms for large-scale distributed sensor networks,” *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006, ISSN: 1550-4859.

[62] Roberto Di Pietro and Luigi V. Mancini and Alessandro Mei, “Random key-assignment for secure wireless sensor networks,” *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN ’03, pp. 62–71, 2003.

[63] Wenliang Du and Jing Deng and Yunghsiang S. Han and Pramod K. Varshney and Jonathan Katz and Aram Khalili, “A pairwise key predistribution scheme for wireless sensor networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, May 2005, ISSN: 1094-9224.

[64] Leonardo B. Oliveira and Hao Chi Wong and Antonio A.F. Loureiro and Ricardo Dahab, “On the design of secure protocols for hierarchical sensor networks,” *International Journal of Security and Networks*, vol. 2, no. 3-4, pp. 216–227, 2007.

[65] B. Panja and S. K. Madria and B. Bhargava, “Energy and communication efficient group key management protocol for hierarchical sensor networks,” *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, p. 8, Jun. 2006.

[66] Haowen Chan and Adrian Perrig and Dawn Song, "Random key predistribution schemes for sensor networks," *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pp. 197–213, May 2003, ISSN: 1081-6011.

[67] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, ser. SASN '03, Fairfax, Virginia: ACM, 2003, pp. 72–82, ISBN: 1-58113-783-4. DOI: 10.1145/986858.986869. [Online]. Available: http://doi.acm.org/10.1145/986858.986869.

[68] Debiao He and Neeraj Kumar and Jianhua Chen and Cheng-Chi Lee and Naveen Chilamkurti and Seng-Soo Yeo, "Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2013, ISSN: 1432-1882.

[69] Ronald Watro and Derrick Kong and Sue-fen Cuti and Charles Gardiner and Charles Lynn and Peter Kruus, "Tinypk: Securing sensor networks with public key technology," *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '04, pp. 59–64, 2004.

[70] Sana Ullah and Henry Higgins and Bart Braem and Benoit Latre and Chris Blondia and Ingrid Moerman and Shahnaz Saleem and Ziaur Rahman and KyungSup Kwak, "A comprehensive survey of wireless body area networks," English, *Journal of Medical*

Systems, vol. 36, no. 3, pp. 1065–1094, 2012, ISSN: 0148-5598. DOI: 10.1007/s10916-010-9571-3..

[71] F. Delgosha, E. Ayday, and F. Fekri, "Mkps: A multivariate polynomial scheme for symmetric key-establishment in distributed sensor networks," in *Proceedings of the 2007 International Conference on Wireless Communications and Mobile Computing*, ser. IWCMC '07, Honolulu, Hawaii, USA: ACM, 2007, pp. 236–241, ISBN: 978-1-59593-695-0. DOI: 10.1145/1280940.1280992. [Online]. Available: http://doi.acm.org/10.1145/1280940.1280992.

[72] N.-C. Wang and H.-L. Chen, "Improving pairwise key predistribution in wireless sensor networks," in *Advances in Intelligent Systems and Applications - Volume 1: Proceedings of the International Computer Symposium ICS 2012 Held at Hualien, Taiwan, December 12–14, 2012*, R.-S. Chang, L. C. Jain, and S.-L. Peng, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 521–530, ISBN: 978-3-642-35452-6. DOI: 10.1007/978-3-642-35452-6_53. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-35452-6_53.

[73] Bing He and Sugata Joshi and Dharma P. Agrawal and Sun Dongmei, "An efficient authenticated key establishment scheme for wireless mesh networks," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–5, Dec. 2010, ISSN: 1930-529X.

[74] M. T. I. ul Huque, K. S. Munasinghe, and A. Jamalipour, "Body node coordinator placement algorithms for wireless body area networks," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 94–102, Feb. 2015, ISSN: 2327-4662. DOI: 10.1109/JIOT.2014.2366110.

[75] Dongyao Chen and Kyong-Tak Cho and Sihui Han and Zhizhuo Jin and Kang G. Shin, "Invisible sensing of vehicle steering with smartphones," *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '15, pp. 1–13, 2015. DOI: 10.1145/2742647.2742659. [Online]. Available: http://doi.acm.org/10.1145/2742647.2742659.

[76] Stanley F. Chen and Joshua Goodman, "An empirical study of smoothing techniques for language modeling," *Proceedings of the 34th Annual Meeting on Association for Computational Linguistics*, ACL '96, pp. 310–318, 1996. DOI: 10.3115/981863.981904. [Online]. Available: http://dx.doi.org/10.3115/981863.981904.

[77] M. Joa-Ng and I-Tai Lu, "A gps-based peer-to-peer hierarchical link state routing for mobile ad hoc networks," *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*, vol. 3, 1752–1756 vol.3, 2000, ISSN: 1090-3038. DOI: 10.1109/VETECS.2000.851573.

[78] Hae-Sang Park and Chi-Hyuck Jun, "A simple and fast algorithm for k-medoids clustering," *Expert Systems with Applications*, vol. 36, no. 2, Part 2, pp. 3336–3341, 2009, ISSN: 0957-4174. DOI: http://dx.doi.org/10.1016/j.eswa.2008.01.039. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S095741740800081X.

[79] Raymond T. Ng and Jiawei Han, “Efficient and effective clustering methods for spatial data mining,” *Proceedings of the 20th International Conference on Very Large Data Bases*, VLDB ’94, pp. 144–155, 1994. [Online]. Available: `http://dl.acm.org/citation.cfm?id=645920.672827`.

[80] Martin Ester and Hans-Peter Kriegel and Jorg Sander and Xiaowei Xu, “A density-based algorithm for discovering clusters in large spatial databases with noise,” pp. 226–231, 1996.

[81] Nello Cristianini and John Shawe-Taylor, *An Introduction to Support Vector Machines: And Other Kernel-based Learning Methods*. New York, NY, USA: Cambridge University Press, 2000, ISBN: 0-521-78019-5.

[82] Alain Rakotomamonjy, “Variable selection using svm based criteria,” *J. Mach. Learn. Res.*, vol. 3, pp. 1357–1370, Mar. 2003, ISSN: 1532-4435. [Online]. Available: `http://dl.acm.org/citation.cfm?id=944919.944977`.

[83] Miro Enev and Sidhant Gupta and Tadayoshi Kohno and Shwetak N. Patel, “Televisions, video privacy, and powerline electromagnetic interference,” *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS ’11, pp. 537–550, 2011. DOI: `10.1145/2046707.2046770`. [Online]. Available: `http://doi.acm.org/10.1145/2046707.2046770`.

[84] Temitope Oluwafemi and Tadayoshi Kohno and Sidhant Gupta and Shwetak Patel, “Experimental security analyses of non-networked compact fluorescent lamps: A case

study of home automation security," *Proceedings of the LASER 2013 (LASER 2013)*, pp. 13–24, 2013.