INTERNET OF THINGS (IoT) APPLICATIONS WITH

DIVERSE DIRECT COMMUNICATION METHODS

A DISSERTATION IN

Telecommunications and Computer Networking

And

Computer Science

Presented to the Faculty of the University of Missouri – Kansas City

in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

By

KAUSTUBH DHONDGE

M.S., University of Missouri – Kansas City, 2011

Kansas City, Missouri

2016

INTERNET OF THINGS (IoT) APPLICATIONS WITH

DIVERSE DIRECT COMMUNICATION METHODS

Kaustubh Dhondge, Candidate for the Doctor of Philosophy

University of Missouri – Kansas City, 2016

ABSTRACT

Internet of Things (IoT) is a network of physical objects or things that are embedded with electronics, software, sensors, and network connectivity - which enable the object to collect and exchange data. Rapid proliferation of IoT is driving the intelligence in things used daily in homes, workplaces and industry. The IoT devices typically communicate via radio frequency (RF), such as WiFi and Bluetooth.

In this dissertation we deeply analyze the various characteristics of different wireless communication methods in terms of range, energy-efficiency, and radiation pattern. We find that a well-established communication method might not be the most efficient, and other alternate communication methods with the desired properties for a particular application could exist. We exploit radically alternative, innovative, and complimentary wireless communication methods, including radio frequency, infrared (IR), and visible lights, through the IoT applications we have designed and built with those.

We have developed various IoT applications which provide security and authentication, enable vehicular communications with smartphones or other smart devices, provide energy-efficient and accurate positioning to smart devices, and enable energy-efficient communications in Industrial Internet of Things (IIoT).

APPROVAL PAGE

The faculty listed below, appointed by the Dean of the School of Graduate Studies, have examined a dissertation titled “Internet of Things (IoT) Applications With Diverse Direct Communication Methods”, presented by Kaustubh Dhondge, candidate for the Doctor of Philosophy degree, and certify that in their opinion it is worthy of acceptance.

Supervisory Committee

Baek-Young Choi, Ph.D., Committee Chairperson
CSEE Department, School of Computing and Engineering

Cory Beard, Ph.D.
CSEE Department, School of Computing and Engineering

Lein Harn, Ph.D.
CSEE Department, School of Computing and Engineering

Praveen Rao, Ph.D.
CSEE Department, School of Computing and Engineering

Rajeev Shorey, Ph.D.
TCS Innovation Laboratories - Cincinnati

Sejun Song, Ph.D.
CSEE Department, School of Computing and Engineering

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

ACKNOWLEDGEMENTS

An undertaking of this magnitude simply cannot be accomplished by a single person, and it could not be truer in the case of my doctoral research. I shall be forever thankful to my adviser Dr. Baek-Young Choi for her mentoring and nurturing. Her constant encouragement and guidance through all phases of my doctoral and master's student career have been a tremendous source of motivation for me. I appreciate her for all the time she has spent training me (and my lab mates) not only in our research but in a multitude of other related technical and soft skills. If I have to do this all over again, there would be no other researcher that I would choose as my adviser than Dr. Choi.

Special thanks are also due for my committee members. Dr. Sejun Song, who guided and mentored me through my doctoral research. His keen insights and guidance have been invaluable. Dr. Praveen Rao, who always took a keen interest in my well-being as a doctoral student, and mentored me. Dr. Rajeev Shorey, who took me under his wings at TCS Innovation-Labs, and in a short time has become a close friend and mentor. Dr. Cory Beard and Dr. Lein Harn, for their patient and insightful feedback on my research.

I would like to thank Dr. Denis Medeiros and Dr. Jennifer Friend for their mentoring during the UM System - Graduate Student Leadership Development Program, and while I was with the UMKC Doctoral Student Council. I would also like to thank my lab-mates Dr. Hyungbae Park, Dr. Sunae Shin, Dr. Xinjie Guan, and Dr. Daehee Kim for their company during this long journey.

Last, but definitely not the least, I am thankful to my wife Dr. Dhivya Ketharnath who no matter what is always there, rock-solid in my corner.

Thank you all for this wonderful and the happiest chapter of my life, and here's to the future!

CHAPTER 1

INTRODUCTION

We are at a turning point in our society where the world around us is deeply embedded with smart objects that are wirelessly connected to each other and eventually through the Internet. The network of such physical objects or things that are embedded with electronics, software, sensors, and Internet connectivity which enables these objects to collect and exchange data forms the basis for the philosophy of the Internet of Things (IoT).

IoT systems and their application have gained unprecedented popularity and proliferation in recent times. A recent report projects the IoT systems to increase in their economic impact from the current $3.9 trillion to $11.1 trillion a year by 2025 [1]. This significant economic impact is a direct result of connecting over 50 billion devices to the Internet, as shown in Figure 1.1 [117]. One part of this growth focuses on connecting everyday objects being used by humans to the Internet. The potential of creating such Internet connected devices or IoT devices is huge. IoT devices offer various avenues that make human interactions with the machines possible. Some examples of such applications are in the field of healthcare by monitoring the vital signs of a person via wearable devices, home automation, home security, personalized care and products, smart vehicles, etc. While such applications offer a huge potential, the other aspect of IoT

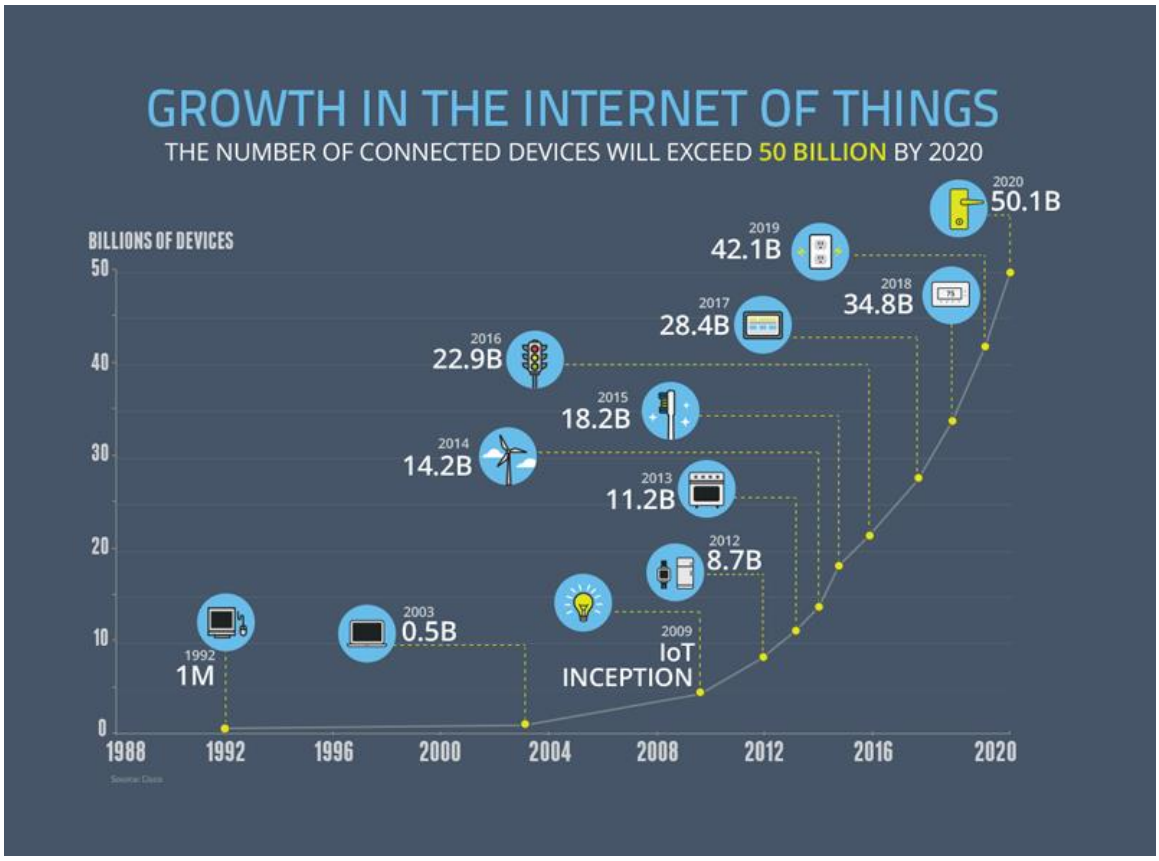


Figure 1. 1: Projected proliferation of the Internet of Things [117]

involves connecting the machines in industries to the Internet, with each other and with the work force in a plant. This philosophy forms the basis for Industrial Internet of Things (IIoT) [2].

At the core of the current IoT technologies, is the communication through radio frequency, such as WiFi, Bluetooth, and cellular data connection. With the prevalence of connected devices, our reliance on the radio frequency communication is becoming

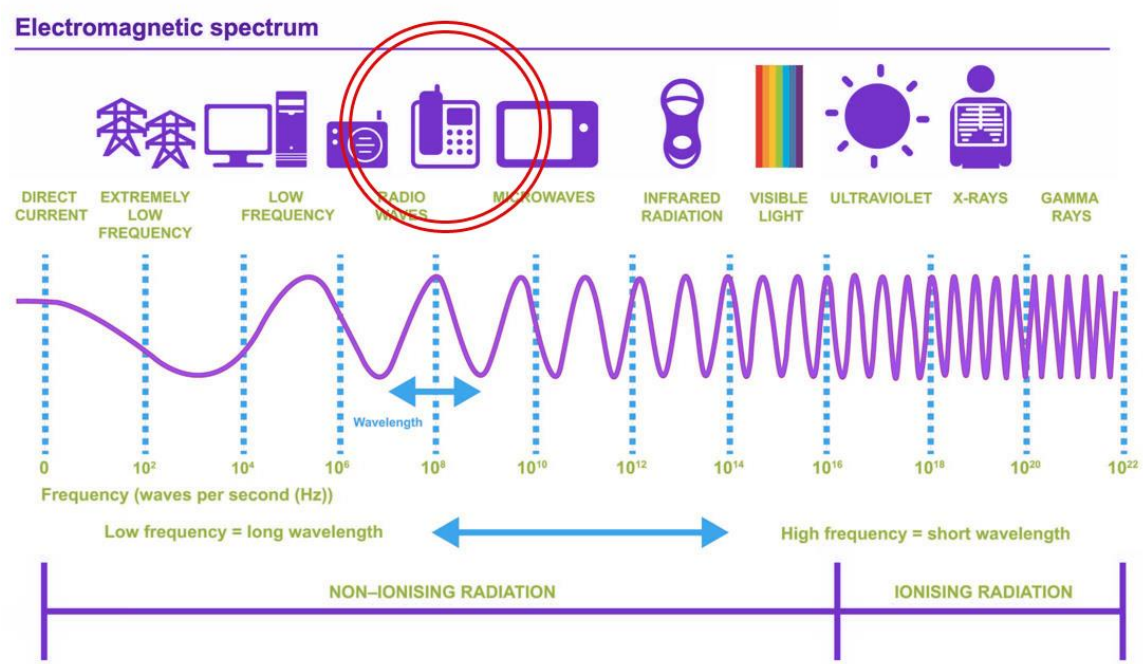


Figure 1.2: The Electromagnetic Spectrum [118]

significant. However, the radio spectrum, which lies in the electromagnetic spectrum as shown in Figure 1.2 [118], is extremely crunched and its dependability becomes a growing issue. Other concerns involve radio frequency smog which not only cause interference in wireless communications, but can also lead to health hazards at high frequencies. As the proliferation of IoT devices in our homes, office spaces and industries grows, and rapidly increasing number of consumers embrace these technologies, the impact of the radio spectrum crunch will be profound, and could become an Achilles heel for the industry.

Therefore, we argue that it is important to diversify the wireless communication methods. In this dissertation, we propose radically alternative, innovative, and complimentary wireless communication methods, including radio frequency, infrared

(IR), and visible lights, through the IoT applications we have designed and built with those. Clever, opportunistic, and collaborative use of the frequencies within the radio frequency spectrum along with other frequencies from the electromagnetic spectrum in general, such as the visible light and infrared radiation, can not only improve the energy-efficiency, speed, and accuracy of the communications, but enable novel applications which could not have been possible with existing RF technologies. We thoroughly analyze and compare their cons and pros from various perspectives with experiments and simulations, and provide insights for a better connected world. In this dissertation, our research contributions are highly interdisciplinary in nature, and involve contributions in the fields of Telecommunications and Computer Networking, Computer Science, as well as Electrical Engineering.

1.1 Dissertation Outline

The rest of the dissertation is structured as follows. In Chapter 2, we describe a novel token-based authentication mechanism for smartphones and other smart devices. As recent smartphone technologies in software and hardware keep on improving, many smartphone users envision to perform various mission critical applications on their smartphones that were previously accomplished by using PCs. Hence, smartphone authentication has become one of the most critical security issues. Due to the relatively small smartphone form factor, the traditional user id and password typed authentication is considered as an inconvenient and time-taking approach. Taking advantage of various sensor technologies of smartphones, alternative authentication methods such as pattern, gesture, finger print, and face recognition have been actively researched. However, those

authentication methods still pose one of speed, reliability, and usability issues. They are especially not suitable for the users in rugged conditions and with physical challenges.

In this chapter of the dissertation, we evaluate existing alternative smartphone authentication approaches in various usage scenarios to propose an ambient light sensor based authentication for smartphones. We have designed and prototyped a challenge-based programmable Fast, Inexpensive, Reliable, and Easy-to-use (FIRE) hardware authentication token. FIRE token uses an onboard LED to transmit passwords via an Optical Wireless Signal (OWS) to the smartphone that captures, and interprets it via its ambient light sensor. FIRE token is a part of the challenge-response technique in the Inverse Dual Signature (IDS) that we designed to facilitate a multi-factor authentication for the mission critical smartphone applications. Together they provide the Optical Wireless Authentication (OptAuth) for the user of the smartphone. Our experiments validate that OptAuth can authenticate a user on a smartphone in a simple, fast, and reliable way without compromising the security quality and user experience [3].

In Chapter 3 of this dissertation, we discuss about our research on vehicular communications to prevent collisions between pedestrians and vehicles. As smartphones gain their popularity, vulnerable road users (VRUs) are increasingly distracted by activities with their devices such as listening to music, watching videos, texting or making calls while walking or bicycling on the road. In spite of the development of various high-tech Car-to-Car (C2C) and Car-to-Infrastructure (C2I) communications for enhancing the traffic safety, protecting such VRUs from vehicles still relies heavily on traditional sound warning methods. Furthermore, as smartphones continue to become highly ubiquitous, VRUs are

increasingly oblivious to safety related warning sounds. A traffic accident study shows the number of headphone-wearing VRUs involved in roadside accidents has increased by 300% in the last 10 years. Although recently a few Car2Pedestrian-communication methods have been proposed by various car manufacturers, their practical usage is limited, as they mostly require special communication devices to cope with the wide range of mobility, and also assume VRUs' active attention to the communication while walking.

In this chapter of the dissertation, we propose a smartphone-based Car2X-communication system, named WiFi-Honk, which can alert the potential collisions to both VRUs and vehicles in order to especially protect the distracted VRUs. WiFi-Honk provides a practical safety means for the distracted VRUs without requiring any special device using WiFi of smartphone. WiFi-Honk removes the WiFi association overhead using the beacon stuffed WiFi communication with the geographic location, speed, and direction information of the smartphone replacing its SSID while operating in WiFi Direct/Hotspot mode, and also provides an efficient collision estimation algorithm to issue appropriate warnings. Our experimental and simulation studies validate that WiFi-Honk can successfully alert VRUs within a sufficient reaction time frame, even in high mobility environments [4].

In Chapter 4, we have developed a collaborative positioning system for smart devices which provides them with accurate location information at a fraction of the energy cost as compared to the traditional positioning approaches. The fast growing popularity of smartphones and tablets enables us to use various intelligent mobile applications. As

many of those applications require position information, smart mobile devices provide positioning methods such as Global Positioning System (GPS), WiFi-based positioning system (WPS), or Cell-ID-based positioning service. However, those positioning methods have different characteristics of energy-efficiency, accuracy, and service availability.

In this chapter, we present an Energy-Efficient Collaborative and Opportunistic Positioning System (ECOPS) for heterogeneous mobile devices. ECOPS facilitates a collaborative environment where many mobile devices can opportunistically receive position information over energy-efficient and prevalent WiFi, broadcasted from a few other devices in the communication range. The position-broadcasting devices in ECOPS have sufficient battery power and up-to-date location information obtained from accurate but energy-inefficient GPS. A position receiver in ECOPS estimates its location using a combination of methods including received signal strength indicators and 2D trilateration. Our field experiments show that ECOPS significantly reduces the total energy consumption of devices while achieving an acceptable level of location accuracy. ECOPS can be especially useful for unique resource scarce, infrastructure less, and mission critical scenarios such as battlefields, border patrol, mountaineering expeditions, and disaster area assistance [5].

In Chapter 5, we work towards improving the operational efficiency of Industrial Internet of Things (IIoT) systems. Internet of Things (IoT) promises to be a key enabler for Smart Manufacturing and Smart Supply Chain. The IoT systems are responsible for enabling and improving the operational efficiencies of factories, plant floors, including assembly plants. These systems are characterized by reliable sensing and reporting of

multiple parameters within the factory floor. Such sensing activities offer safe, efficient and optimized performance of not only the machines manufacturing the products, but also the workforce operating them. Industrial IoT (IIoT) systems could suffer from high and unbalanced energy consumption due to the nature of the network deployment. Such behavior is undesirable as it not only increases the carbon footprint of the plant, but also makes the planned maintenance of IoT devices for battery replacement a huge challenge.

In this chapter, we propose a heuristic and opportunistic link selection algorithm, HOLA, which not only reduces the overall energy consumption of the IoT network but also balances it across the network. HOLA achieves this energy-efficiency by opportunistically offloading the IoT device data to smart-devices being carried by the workforce in the factory settings. Further, these smart-devices with multiple radio links such as Bluetooth, Wi-Fi, and 3G/4G LTE heuristically determine the best link to transmit the data to the Cloud based on the quality and energy cost of the link. Our experimental and simulation studies validate that HOLA can improve the energy efficiency of IIoT systems by reducing the overall energy consumption and balancing it across the network [6].

In Chapter 6, we work towards the development of a secure, electronic smart door lock. The recent advancements in Internet of Things (IoT) have spurred an unprecedented revolution of connecting various everyday use objects to the Internet. One such application is that of Smart Door Locks (SDL). While electronic door locks have been used in the enterprise for close to four decades, this revolution in the IoT coupled along with the proliferation of smartphones has been responsible for spurring the recent adoption of SDL for home and other commercial use. The SDL are an attractive replacement to

traditional door locks as they offer increased security, and easy key sharing while offering ease of operation.

In this chapter, we propose an optical wireless unlocking for SDL. We have designed and prototyped a SDL system named OptLock. OptLock accepts an optical wireless signal (OWS) which contains the encoded one-time-password (OTP) key via its onboard infrared (IR) sensor to unlock. This challenge-response based OWS is transmitted by the user through a smartphone via its onboard IR light emitting diode (LED). In the absence of an onboard IR LED, an external dongle containing an IR LED can be easily connected to the smartphone. This hardware we designed is powered though the smartphone's 3.5 mm headphone jack. Our experiments and analysis validate that OptLock offers a fast and efficient unlocking experience which is highly secure, and successfully thwarts various attack scenarios [7].

In Chapter 7, we conclude this dissertation with a summary of our contributions. We discuss about the possible future work, and research directions that could arise from our research presented in this dissertation to enable a better connected world with the Internet of Things.

CHAPTER 2

OPTICAL WIRELESS AUTHENTICATION FOR SMART DEVICES USING AN ONBOARD AMBIENT LIGHT SENSOR

As smartphones gain their remarkable popularity, and their technologies in software and hardware keep on improving, they are envisioned eventually to be functional as primary devices for various mission critical tasks previously accomplished with PCs. Considering that a great portion of the online services requires various types of client and server authentications, in addition to the access of the smartphones itself, smartphone users will be requested to do authentication as many times as PC users do. However, smartphone's small screen and keypad make it challenging for users to use the traditional user id and password typed authentication method whenever access to the device as well as the services are needed. It can be especially difficult for the users in rugged conditions or with physical challenges. For example, in addition to the personal usage, government agencies including DARPA, ARL, and NSA have been actively seeking smartphone technologies to support various DoD mission critical activities, including the tactical battlefield mission, disaster recovery, and other mission areas. Soldiers in a battlefield during covert surveillance missions or people with difficulties in fine motor controls may not be able to type in the right passcode in a timely manner. Additionally, there is a growing traction among the experts in the security field that days of simple password based systems are over [8] since they are easily guessed, cracked, and stolen.

Taking advantage of various sensor technologies of smartphones, alternative authentication methods such as a pattern, gesture, fingerprint, and face recognition have been actively researched. Authentication techniques can be classified into four categories as follows:

- Something that a user knows (user-know): This constitutes techniques such as passwords, pin codes, and patterns that can be drawn.
- Something that a user is (user-is): This constitutes biometric traits of a human body such as their fingerprints, face, and iris as well as environments such as location and orientation that are unique to the particular person.
- Something that a user does (user-do): This constitutes an activity that only a particular person can generate such as its handwritten signature, gestures, and voice generation.
- Something that a user has (user-have): This constitutes a secure and unique hardware token that is possessed by the owner alone.

Although many smartphone authentication methods have been developed to optimize speed and usability while being secure and reliable, they still pose one of security, speed, reliability, and usability issues. For example, Knock Code [9] that uses a knocking pattern to unlock a phone was introduced by LG in 2014 MWC (Mobile World Congress). Although it improves usability, the security level is the same as the original pattern-based authentication. Several alternative biometric approaches [10], [11] have been proposed mainly as a second factor authentication to heighten the security level. However, biometric based authentication techniques can be computationally expensive,

and moreover are hard to replace once their security is compromised. Camera-based facial recognition may not work for a soldier applying a camouflage to her face, or in a dark environment. Recent sensor-based authentication techniques [12], [13], [14] use location, orientation, adjacency-to-token, or magnetic information. However, the reliability of those authentication techniques is susceptible to environments such as noise and signal jamming. Especially, communication sensors such as WiFi or Bluetooth tend to consume relatively high energy and require a longer negotiation time.

In this work, we evaluate existing alternative smartphone authentication approaches in various usage scenarios, and propose ambient light sensor based Fast, Inexpensive, Reliable, and Easy-to-use (FIRE) authentication for smartphones. We leverage ambient light sensors that are already available in most smartphones. An authentication to unlock a smartphone and/or to enable web or cloud service access can be done using a light-emitting token. The light-emitting token is programmable by using configurable challenges via a small and inexpensive encoder. FIRE falls under the category of user have and user know while combining the two authentication paradigms to deliver a multi-factor authentication technique. A multi-factor authentication scheme inherently tends to be more secure over single-factor authentication schemes.

We designed and prototyped the FIRE hardware token which uses an onboard LED to transmit a programmed authentication key bit string via an Optical Wireless Signal (OWS) to the smartphone. The smartphone captures and interprets this OWS via its ambient light sensor providing the Optical Wireless Authentication (OptAuth) for the user of the smartphone. The experimental results validate that the proposed light sensor token

method can achieve FIRE smartphone authentication without compromising the security quality. The token can be eventually designed and carried in various inexpensive and small form factors including a key chain, a ring, and smartphone accessories. Our major contributions in this work consist of 1) evaluating smartphone centric authentication methods; 2) proposing a light-emitting token based FIRE smartphone authentication technology; 3) proposing a Challenge-Response and Inverse Dual Signature (IDS) security scheme; and 4) prototyping and validating the feasibility of the proposed authentication method.

The rest of this chapter is organized as follows. A detailed explanation of the proposed OptAuth system is presented in Section 2.1. The prototype implementation along with performance evaluations and experimental scenarios are explained in Section 2.2. Section 2.3 discusses the existing and state-of-the-art authentication techniques. Finally, we conclude the chapter in Section 2.4.

2.1 OptAuth Approach

A light sensor is one of the most common sensors in smartphones, and is located on its surface above the screen. Since the screen of a smartphone is a major factor in draining its battery, an ambient light sensor is used to recognize the brightness of its surroundings and adapt the screen backlight to save battery power while optimizing the visibility. We exploit the existing and prevalent light sensor in smartphones and use a programmable light token generator for the authentication. A light emitter can be a small portable token

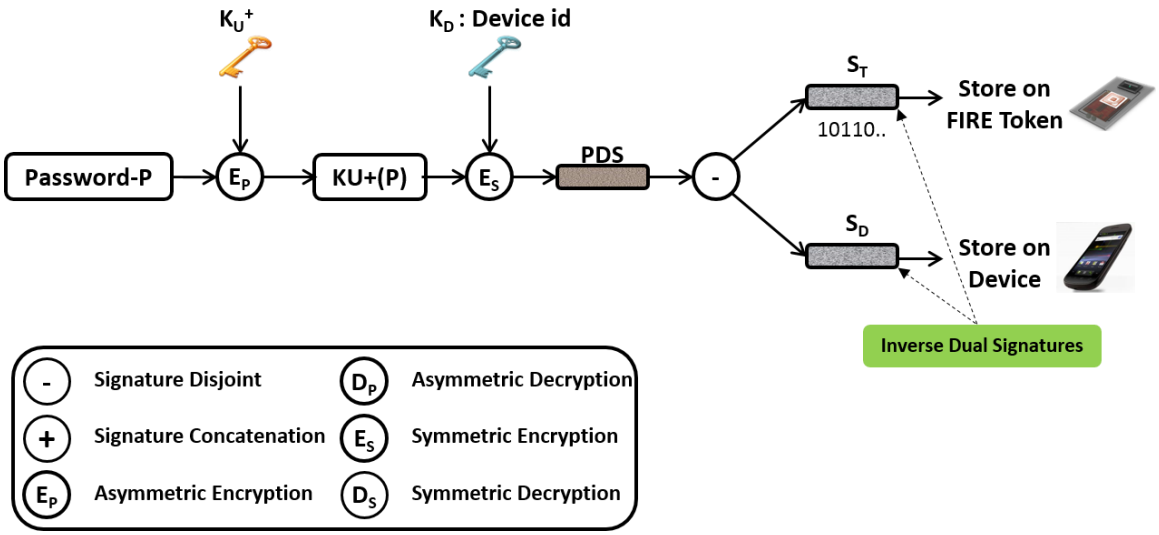


Figure 2. 1: OptAuth: Key storing phase

embedded into everyday objects such as a key chain, a security badge, and smartphone accessories. A FIRE hardware token consists of battery powers, a microcontroller, a light source LED, a photoresistor sensor [15], a guard around the LED, programmable code key buttons, and optionally an NFC chip. An NFC chip can be used for a multi-factor token. It ensures the proximity of the FIRE token to the authenticating smartphone as well as stores the authentication for multiple server accesses. Multiple types of authentication information on the NFC chip can be selected from a drop-down menu when scanned by the smartphone.

We propose an Inverse Dual Signature (IDS) security scheme to complement the OptAuth approach. In SET (Secure Electronic Transaction) [16], the concept of Dual Signature is used by concatenating two different pieces of information to generate a

Algorithm 2. 1: FIRE Key Store Phase

FIRE – KeyStore Phase
1: encrypt password with CAs public key K^{+}_{U} ;
2: K^{+}_{U} is passed through symmetric encryption function E' with device IMEI as key K_D to generate Password Device Signature PDS;
3: disjoin PDS into Token Signature S_T , and Device Signature S_D;
4: S_T is stored on the FIRE token;
5: S_D is stored on the mobile device;

single message digest, which, after encryption with the user's private signature key results in a Dual Signature. In this work, we take an inverse approach, where we disjoin a single piece of information which is user's password, and encrypt it with CA's public key followed by user's symmetric key. This results in two signatures that are intended for the FIRE token, and the user's smartphone, respectively.

An OptAuth smartphone authentication approach takes the following process. First, as illustrated in Figure 2.1, the user's password is encrypted with Certificate Authority's (CA) public key (K^{+}_{U}) for the user. This is further encrypted with symmetric encryption function E' that takes the smartphone's IMEI as its key to produce the Password Device Signature PDS. A disjoin function breaks PDS into Token Signature S_T and Device Signature S_D. While S_T is stored on the user's FIRE token, S_D is stored on user's smartphone as shown

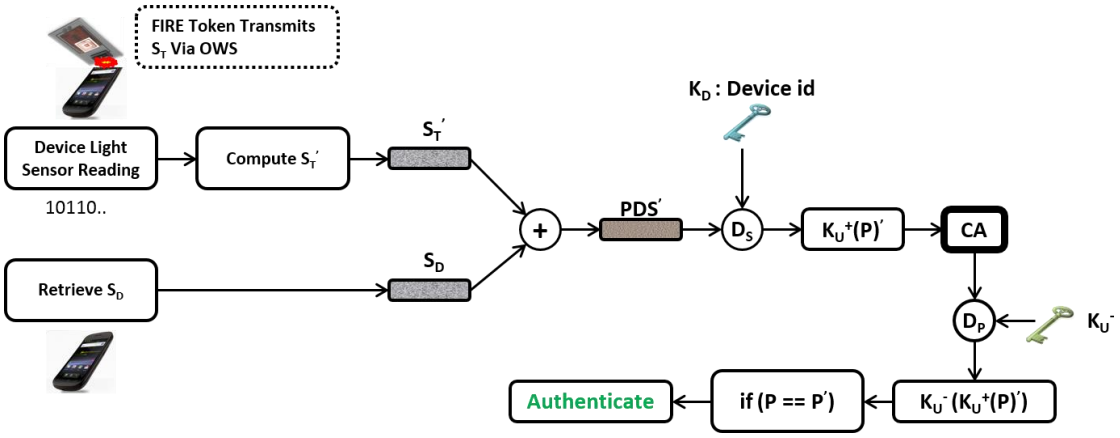


Figure 2. 2: OptAuth: Authentication phase

in Algorithm 2.1. Using a device unique information such as IMEI to encrypt K^+_U generates a PDS that only the specific device can recover by decrypting it with the IMEI as the key again. In absence of the IMEI for a device, its MAC address can be used.

Additionally, we have designed a unique challenge-response technique to aid in ensuring that the holder of the FIRE token is the actual owner of that FIRE token. This technique is critical to guard the smartphone owner against the security threat in which both the smartphone and FIRE token are stolen by the same attacker. It is also essential for the entire challenge-response and authentication process to be touchless and typing free to maintain a high usability in emergent scenarios where smartphones are being used by soldiers in battlefields, and patients with difficulties in their fine motor controls.

During the challenge setting phase as illustrated in Figure 2.3, the user is presented with a random collection of color patterns on the smartphone screen. The user must select one of those color patterns as the challenge for authentication by pressing the

Figure 2. 3: OptAuth Challenge setting phase

particular tile. Then the user must scan this color pattern with the photoresistor sensor embedded on the surface of the FIRE token (not implemented yet). The FIRE token registers the scanned color pattern RGB from the photoresistor sensor.

During the authentication phase the user must first prove that he/she is the actual owner of that smartphone, and FIRE token. This is achieved using the challenge-response scheme as illustrated in Figure 2.4. The user is first presented with a random collection of color patterns on the smartphone screen in which a few patterns along with the actual challenge always repeat. The user then scans the required color pattern from the screen with the photoresistor sensor embedded on the surface of the FIRE token. The FIRE token registers the sensor readings from the photoresistor and computes it as RGB'. If the values of the scanned RGB', and the set value of the challenge RGB match, then the FIRE token is activated to transmit the user's password.

Then as illustrated in Figure 2.2 and Algorithm 2.2, the user employs the FIRE token to transmit S_T via OWS. The smartphone ambient light sensor interprets the variation in light frequency of OWS to compute S'_T. The smartphone then retrieves S_D from its memory. A concatenation function then results in the recovery of PDS'. The device then

Algorithm 2. 2: Fire - Authentication phase

FIRE – Authentication Phase

1: user places FIRE token on smartphone light sensor, transmits S_T via Optical Wireless Signal (OWS);

2: smartphone light sensor interprets variation in light frequency of OWS to compute S'_T;

3: smartphone retrieves S_D stored in its memory;

4: concatenate S'_T and S_D to obtain PDS : PDS = (S'_T+S_D);

5: smartphone reconstructs K^+_U (P) = D'(PDS);

6: symmetric decryption function D' uses device IMEI as key to recover K^+_U (P);

7: User provides K^+_U (P) to CA for authentication;

8: CA uses its private key to decrypt password from User: P = K^-_U (K^+_U (P))

9: if P == P' then

10: user successfully authenticated;

11: end if

12: if P != P' then

13: user authentication is unsuccessful;

14: notify user of possible attempted unauthorized access by trusted mechanism;

15: end if

reconstructs the encrypted password K^+_U (P) by running PDS' through symmetric decryption function D0 that requires the device IMEI as the key. The user then provides

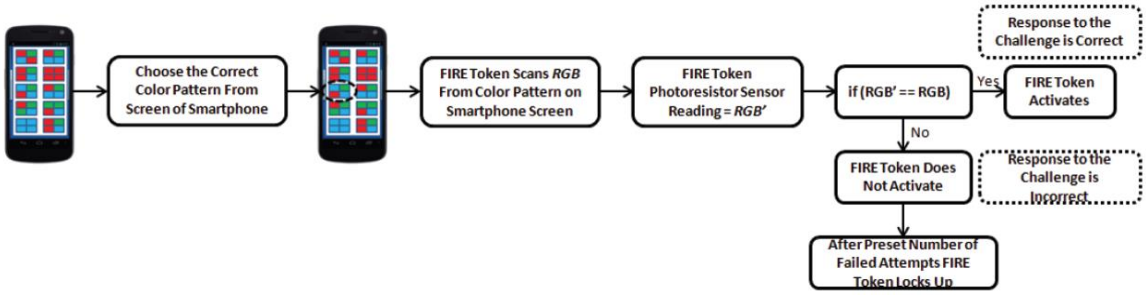


Figure 2. 4: OptAuth Challenge-response phase

the CA with K^{+}_{U} (P) for authentication. The CA in turn decrypts K^{+}_{U} (P) with its private key for the user K^{-}_{U} to obtain P'. If P' and the user's allocated password P match, then the user is successfully authenticated as illustrated in Figure 2.5.

If the values of RGB' and RGB do not match, the FIRE token perceives that an attacker is trying to access the token, and does not activate further to transmit the password. After a predetermined number of failures to identify the correct challenge, the FIRE token locks up altogether to thwart any misuse of the FIRE token. Let p be the probability of an adversary to randomly guess the challenge-response. In addition, suppose t and c are a preset limit of trials and the number of color patterns on the screen, respectively. Then, p can be calculated by

$$p = \frac{t}{c}$$

The number of color patterns, c, is a function of m and f as below:

$$c = \prod_{i=0}^{m-1} f - i$$

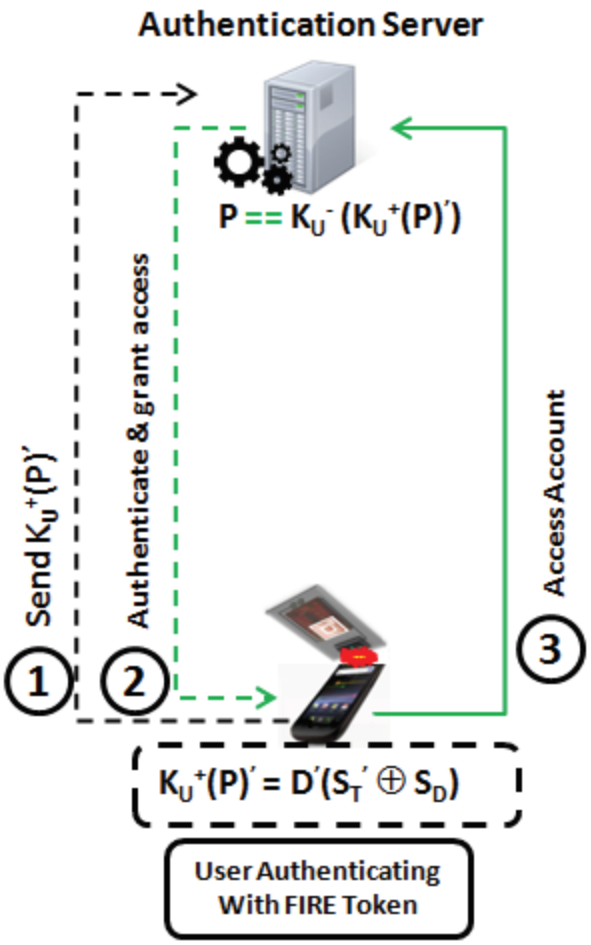


Figure 2. 5: FIRE approach: Successful user authentication example

where m is the number of tiles in one color pattern and f is the number of colors. We assume f is greater than or equal to m. As the passcode of the user is encrypted twice, and only one half of it is kept on the FIRE token, it is practically impossible for the attacker to guess the correct password by a brute-force attack on the FIRE token hardware.

The proposed IDS scheme along with the challenge response scheme and FIRE token offer high security and defeat various attack models associated with hardware token based security approaches as follows:

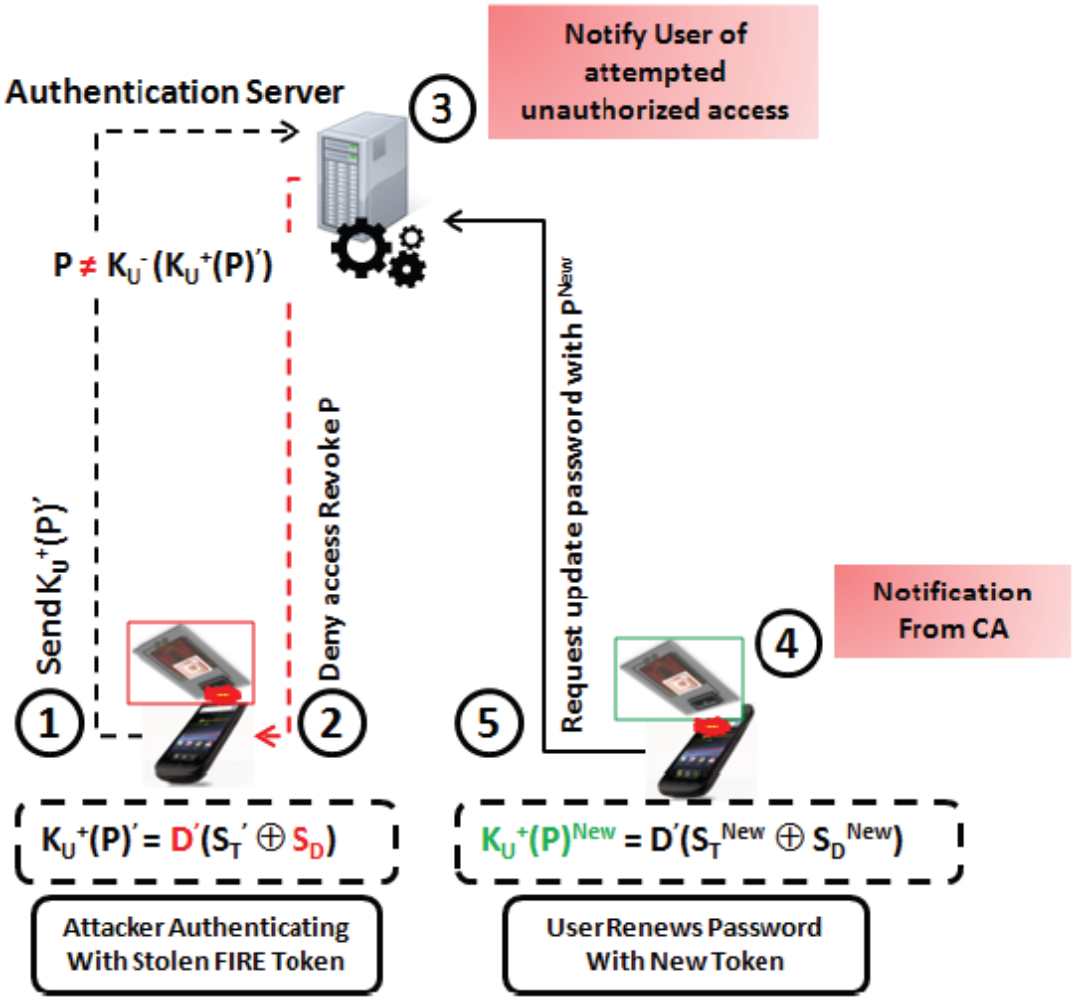


Figure 2. 6: FIRE approach: Unsuccessful attacker authentication example

- Stolen FIRE Token and Smartphone: If the user's FIRE token, and smartphone are stolen by the same attacker, the attacker is unable to access the user's accounts as the attacker is unaware of the correct response to the color pattern challenge. So as the attacker is not able to scan the RGB' value from the color pattern that will match the RGB value that the FIRE token is

Table 2. 1: Comparison of various authentication techniques

Authentication Technique	Time (sec)	Security Level	Summary
Username & Password	~24.5	High	Hard to enter complex passwords
Username & Password while wearing gloves	~45.5	High	Trouble with responsiveness of touch screen
Fingerprint recognition (including time to take gloves off)	~2	Moderate	Low recognition rate with foreign substances on fingers, unusable when wearing gloves
Facial recognition	~2	Moderate	Unusable for face with camouflage, protective eyewear or helmets, dim lighting
Patterns	~1	Low	Easy to break
Fire	~1	High	Fast, Inexpensive, Reliable, and Easy-to-use

expecting, the FIRE token will not activate to send the passcode via OWS. Additionally, after a preset number of wrong attempts at the challenge-response, the FIRE token will lock itself from further use.

- Stolen FIRE Token: If the user's FIRE token gets stolen, the attacker is incapable of producing correct K^{+}_{U} (P) to offer to the CA. This is because the attacker lacks S_D that is stored on the original user's smartphone. So when the attacker tries to present the CA with K^{+}_{U} (P) by using a stolen token, it results in failed authentication as illustrated in Figure 2.6. The user is further notified of this event, and a new password and FIRE token are issued. In case the user's smartphone and FIRE token both are stolen, the CA issues a new password and FIRE token for the user.

- Snooping OWS from the FIRE Token: The attacker's attempts to snoop on the bit stream of OWS from the FIRE token are defeated by multiple factors. First, the physical guard around the light emitter blocks snooping attacks apart from enabling the isolation of environmental light that aids in better sensor reading. Second, the attacker is unable to reproduce correct K^{+}_{U} (P) due to lack of S_D and also the IMEI number of the smartphone that is unique to a particular phone.

Therefore, the probability (p") of correct authentication of an adversary can be summarized as follows:

$$p" = \frac{t}{c}, if\ both\ FIRE\ Token\ and\ Smartphone\ are\ stolen$$

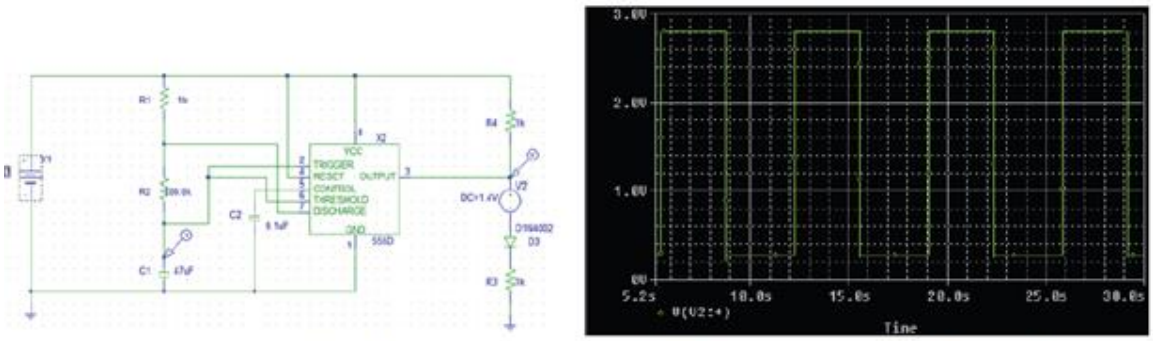
$$p" = 0, if\ only\ FIRE\ Token\ is\ stolen$$

$$p" = 0, if\ snooped$$

OptAuth provides authentication services for a variety of usage scenarios such as unlocking the smartphone or authentication for online services such as banking, emailing, and social networking. For the case of unlocking the smartphone, there is no need for the device to be connected to the network. The challenge-response step will be followed by IDS, and the passcode for it can be stored locally on the smartphone. For services such as banking, emailing, and social networking the smartphone will need to be connected to a network to access those services, and also to verify the authenticity of the user with the particular service provider's authentication servers.

As presented in Table 2.1, we have tested the processing speed of various smartphone authentication methods and compare and summarize the performance and security level. According to the aforementioned characteristics, we discuss the advantages of the FIRE authentication approach as follows:

- Fast: Using a light token only requires a proximity to the smartphone's light sensor instead of manually typing user name and password that is especially hard in challenging environments. Hence, it enables the faster authentication than the traditional approaches. As also shown in Table I, FIRE is faster than other alternative authentication approaches such as facial recognition and fingerprints. FIRE's authentication speed is the fastest and as good as the pattern based authentication.
- Inexpensive: The cost of building a light token hardware is less than $4 in our prototype implementation, as described in Section 2 of this chapter. The cost can be even lowered with mass production.
- Reliable: A smartphone's light sensor reading is a highly accurate and straightforward technology compared to other sensor technologies. We validate this by using our simple and inexpensive LED prototype. For example, magnetic sensors or microphones [14] would pick the magnetic fields and background noise that are commonly present in the environment, requiring special filtering techniques. Other token based alternative authentication approaches can typically address the threat of unauthorized access and a device theft by blocking the access without the token. In addition, a high



(a) Timer circuit design in PSpice (b) Output for timer circuit design in Pspice

Figure 2. 7: Timer circuit design and LED output in PSpice simulator

proximity contact and a guard around the token light emitter isolate its signal from interference or noise and exclude snooping threats. Furthermore, an Infrared (IR) LED can be embedded in the token that is invisible to human eyes.

- Easy-to-Use: Unlike most biometric authentication approaches, it can be easily used in a dark environment, and does not require cumbersome typing. An easy authentication is critical for the users in disaster or military environments, or for those with physical challenges or disabilities.

2.2 OptAuth Prototype Implementation and Evaluation

In this section we explain the implementation and experimental settings used to validate the feasibility of employing a smart device light sensor for authentication.

We have built a simple circuit that is able to modulate a digital bit string into a sequence of lights toggling on and off for a controlled time interval. The time should be brief enough to transfer the bit string in a short time and not be easily detected by human

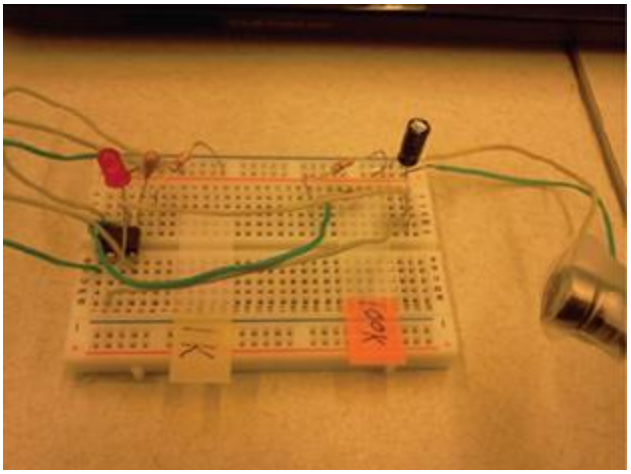


Figure 2. 8: Timer circuit prototype implementation

eyes. The light sequence also includes a few bits of (e.g., 10101) a preamble for synchronization in addition to the secure authentication bit string. We have used the HTC One (M8) smartphone powered with Android 4.4 for all the experiments, and wrote our OptAuth application with the Android SDK. While profiling the ambient light sensor of the smartphone, we employed an application AndroSensor [17] additionally to capture the ambient light sensor readings for sanity check.

We first experimented to see if the light sensor on the smartphone was capable of distinguishing various bit patterns encoded with light emitters. For this purpose, we modeled the timer circuit in PSpice simulator shown in Figure 2.7, and then designed a prototype circuit with hardware components, Figure 2.8. We observed that the simulated and generated light waveforms matched with the actual sensor readings on the smart devices.

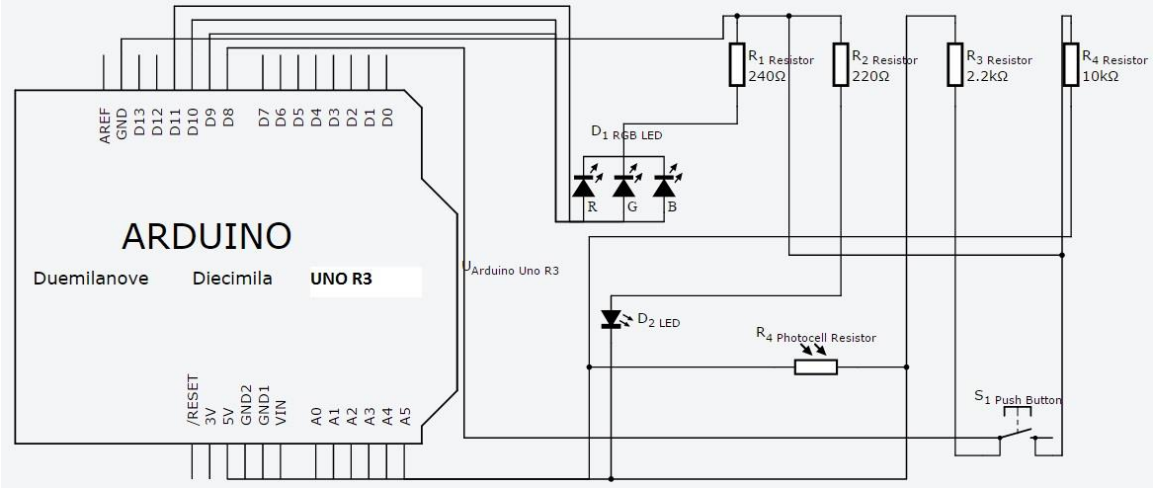


Figure 2. 9: FIRE token circuit implementation

We then built and programmed a prototype light encoder hardware using the ultra-low power microcontroller ATmega328P by Atmel [18]. The ATmega328P microcontroller was programmed using the Arduino Uno Revision 3 [19] microcontroller board. The schematic of the circuit we built for the FIRE hardware token along with the block diagram of the Arduino Uno microcontroller board is shown in Figure 2.9 and the hardware token we built is shown in Figure 2.10. The size of this board is smaller than a credit card and the total retail price of the light encoder and emitter components was only about $2 that would become even smaller with mass production. The cost is by far lower compared to other available tokens such as RSA SecurID [20] or VASCO Digipass [21] that cost around $50. We have use the bread board to attach additional components to the Ardunio Uno microcontroller. In practice, however, this can be compactly packaged into a key chain, a ring or other smartphone accessories. The latest version of the hardware token we built

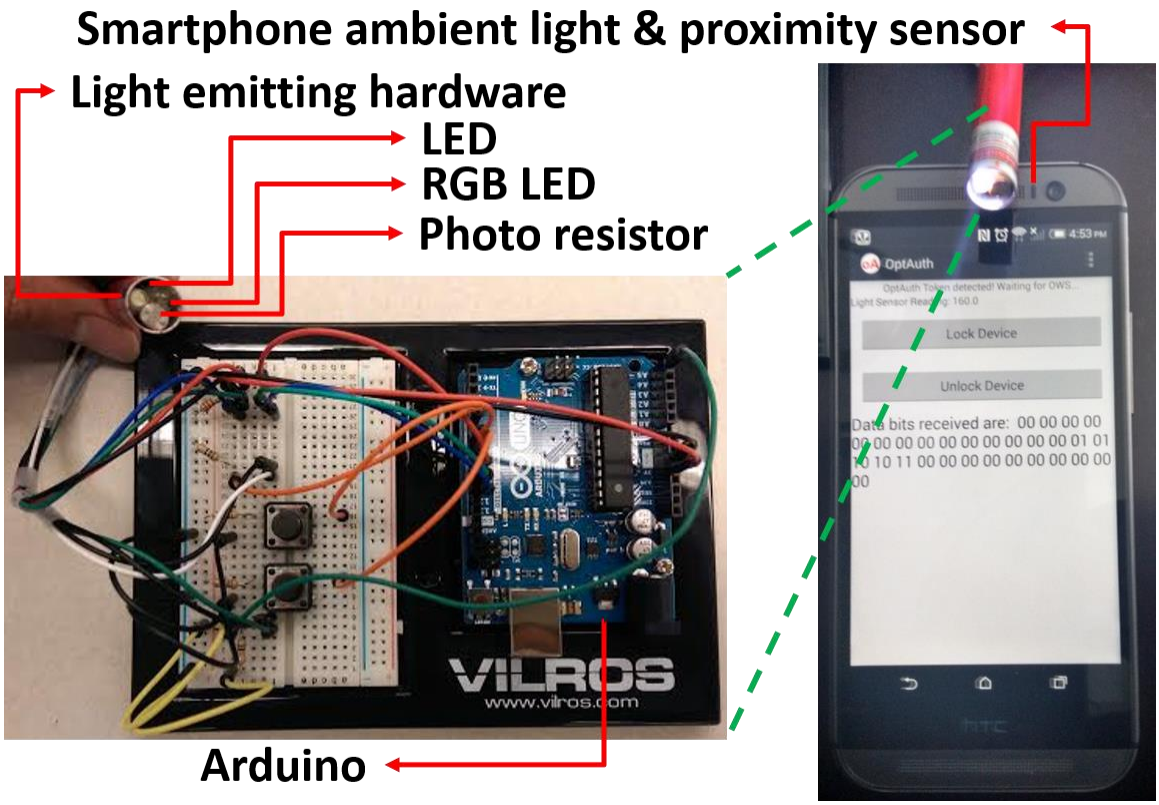


Figure 2. 10: FIRE token hardware set up with Arduino Uno

is shown in Figure 2.11. It is built with an Arduino Nano which again has an ATmega328P microcontroller, and is designed as a compact wearable type of device.

We built the OptAuth application for Android using the Android SDK. The application has been designed to listen for the OWS via its ambient light sensor once it detects the presence of the FIRE token. The OptAuth application perceives the presence of the FIRE token when its proximity sensor (which is collocated with the ambient light sensor) is triggered, and continues to register the presence. The application also displays various

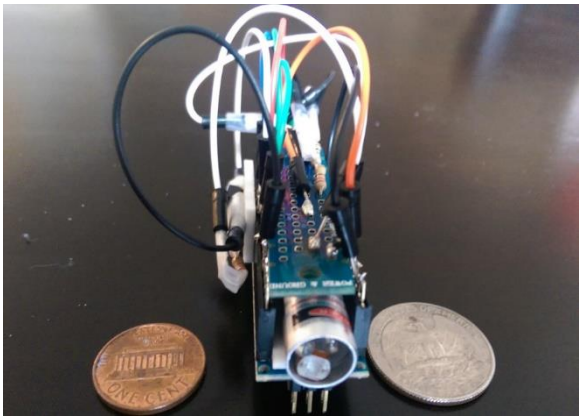
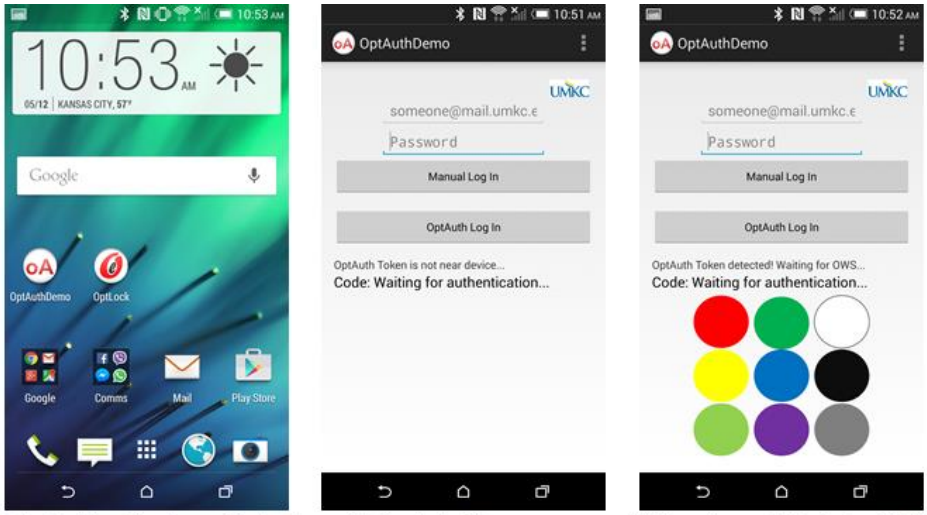


Figure 2. 11: FIRE token hardware setup with Arduino Nano

status messages, and displays the bit string that was received from the FIRE token. The screenshots for the application are shown in Figure 2.12.

Next, we verify the viability of using the ambient light sensor of a smartphone to receive an OWS that is transmitted by the OptAuth token experimentally. We first profiled the ambient light sensor on the HTC One (M8) smartphone to observe its sensitivity to various light levels. The LED connected to the microcontroller in the token can have varying levels of brightness by varying the value of analogWrite function that uses the Pulse Width Modulation (PWM) available on certain digital output pins. This analogWrite value can be varied between 0 and 255 with steps of 1. The corresponding values of brightness (in lux) that are recorded by our OptAuth application are shown in Figure 2.13. To verify the correctness of our application, we have compared it with a commercially available application, AndroSensor. As can be seen from the Figure 2.13, both the application record nearly similar values of lux for corresponding brightness of the token



(a) Android applications - OptAuth (b) OptAuth Home screen (c) Scanning and displaying OWS

Figure 2. 12: OptAuth android application screenshots

LED. These various levels of brightness can also be observed from Figure 2.14. It should be noted that for a high data rate, the LEDs switching rate from one state to another becomes so high that it appears as a flicker to the human eye, and it is impossible to discern the data being sent by just observing.

For the OptAuth technique to be fast and reliable, the FIRE token should be able to send the key bit string that is long enough for strong security at a very high data rate with no or minimum errors. For this we first aim to understand the physical data rate limits of the ambient light sensor of the smartphone using a basic modulation scheme such as ON-OFF keying (OOK), and then device a more sophisticated modulation scheme for achieving relatively very higher data rates.

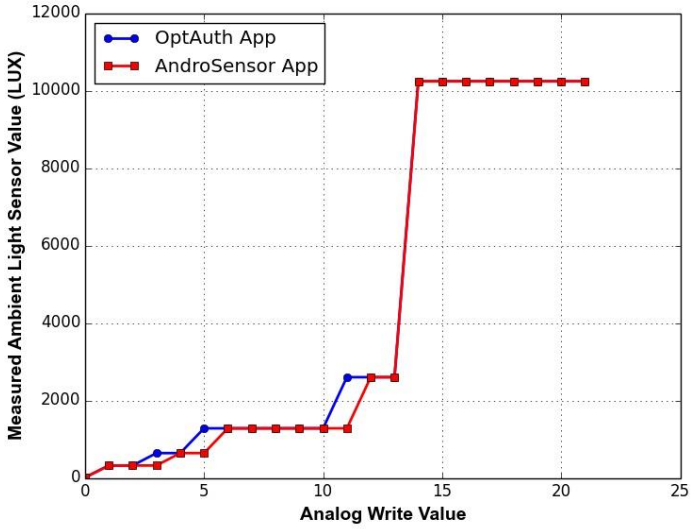


Figure 2. 13: Android ambient light sensor sensitivity to brightness of FIRE token

The Android KitKat operating system (4.x) can scan its sensors at four predefined levels, and specifically reports the new value of the ambient light sensor when it changes. Otherwise, the sensor retains the stale value. These four delay types that can be set are Fastest, Game, UI, and Normal in the increasing order. A detailed comparison of these delay types, their sensing delays, and corresponding energy efficiency is shown in Table 2.2.

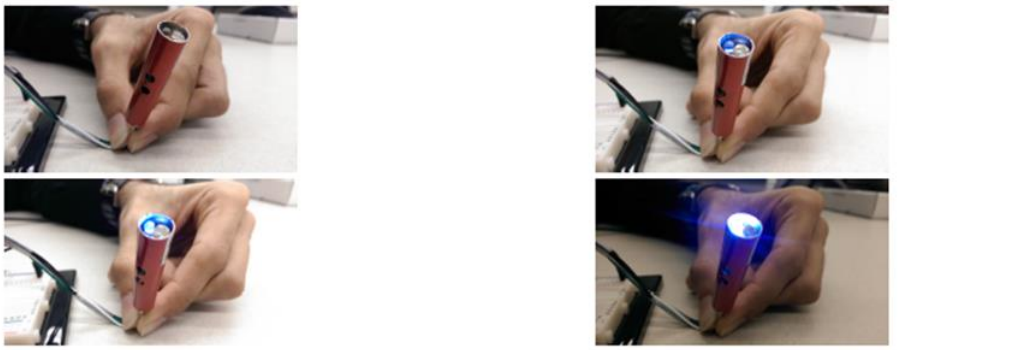
We find that the with the sensor delay set to the Fastest rate, i.e. reporting the change in the lux values with zero delay, the minimum switching period between two consecutive states of the LED has to be at least that of 3 msec. That is, the minimum width of the pulse has to be at least that of 3 msec for OOK. Based on this, experimentally we could achieve a data rate of 333 bits/sec for OOK with zero errors. The OOK modulation scheme is

shown in Table 2.3. The ON symbol indicates that the LED is emitting light, and the OFF symbol indicates that the LED is not emitting light. The data rates that can be achieved for the other Android sensor delay levels are shown in Figure 2.15.

Now, another interesting information that can be perceived from Figure 13 is that there are exactly six different levels of lux values that are recorded. Thus we used the difference between the six different lux values to create more levels to represent the bits. If we use the six levels as is we can have only 2-bit representation at the max (00 to 11) due to the 2^2 i.e. four unique values available at the max to fit the 2^x representation.

To get more values for the 6 different lux levels that we can observe, we used the difference between each of them. This combination of differences yields exactly 16 unique values. On the basis of those 16 different values i.e. 2^4 different values we can use 4-bit representation of 0000 to 1111 assigned to each of them. This modulation scheme thus results in 4 times improvement over the base one resulting in total achievable data rate of 1332 bits/sec (or 1.332 Kbps). So for e.g. if we have a 128 bit key, we can still send it via the token in under 1 second, and have additional bits for verifying if it was received correctly by the Android app with some error correcting scheme. We call this modulation scheme for OptAuth as Light Intensity Modulation (LIM) which is shown in Table 2.4.

Note that FIRE can use either ambient light LEDs or infrared LEDs (IR LEDs) for the light sensors in smart devices. While it uses slightly more energy than ambient LEDs, IR LEDs that fall under the far infrared category operate with a 50 ~ 1,000 mm wavelength, and



(a) analogWrite = 0 and LightSensor Reading = 10 Lux (b) analogWrite = 1 and LightSensor Reading = 320 Lux
(c) analogWrite = 6 and LightSensor Reading = 1280 Lux (d) analogWrite = 255 and LightSensor Reading = 10240 Lux

Figure 2. 14: OptAuth FIRE token LED emitter

are not visible to human eyes [22], thus can be more secure without a light guard around the LED. The ATmega328P is a very low power micro controller, and will draw about 34.5 mA or 41 mA while operating an ambient LED and an IR LED, respectively, for 1 ms [23] [24]. The remote key for unlocking a car typically use a CR2025 button battery. This CR2025 can be used to power the micro controller, and it has a capacity of 150mAh [24]. Then, an estimated operation time of a FIRE token can be obtained using the following equation:

$$OperationalTime = \frac{BatteryCapacity}{CurrentDrawn/Operation}$$

The results in an operation time of 3.6585 hours with IR LEDs. Now if the FIRE token is encoding a 10 bit security code at 10 bps, the token can be used approximately 13,170 times on a single battery which can last over 3 years if the FIRE token is used 10 times per

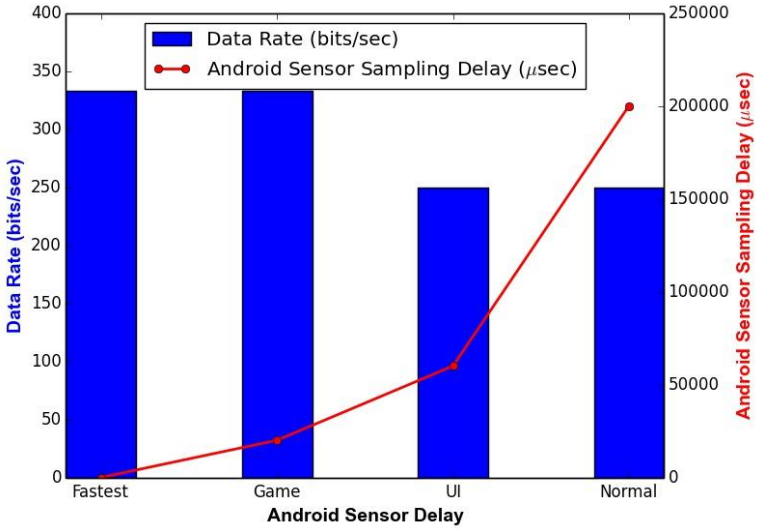


Figure 2. 15: Android light sensor data rates

day. The approximate lifetimes of the FIRE token with various battery types are shown in Table 2.5.

2.3 Related Work

Various authentication approaches can be identified in literature including biometric based, sensor based, and token-sensor based authentication.

Biometric based authentication techniques [10], [11], [25], [26] rely on the uniqueness of certain physical traits in humans. Some of these traits are fingerprints, finger knuckles, retinas, and walking patterns. The major problem of biometric based authentication techniques is that it is hard to replace once their security is compromised. On the other hand, token based authentication schemes can be easily replaced and renewed if they

Table 2. 2: Android sensor delay comparison

Android Sensor Delay	Min Pulse Width (msec)	Data Rate (bits/sec)	Sampling Delay (microsec)	Weighted Android Energy Efficiency
Fastest	3	333	0	~ 0
Game	3	333	20,000	~ 0.1
UI	4	250	60,000	~ 0.3
Normal	4	250	200,000	~ 1

are lost or if their security is compromised. Furthermore, visual face recognition does not work for a soldier applying a camouflage to his/her face, or in a dark environment.

Recently, sensor based authentication techniques [12], [13], [27], [28], [29], [30], [31] have been proposed. They rely on the various sensor readings within a smartphone itself such as the location sensor, and orientation sensor when a smartphone is in use. However, those sensor based authentication techniques are likely to need additional filtering techniques due to the sensitivity of noisy environments. Communication sensors on smartphones such as WiFi or Bluetooth [32] tend to consume relatively high energy and require a longer time due to their own authentication or negotiation. Signal emitters of such RF would also be relatively expensive. Furthermore, such schemes become unusable under electromagnetic pulse (EMP) attacks where wireless communication channels are not available due to signal jamming.

In token-sensor based authentication schemes [14], [33], [34] an additional token such as a QR code, magnetic or acoustic keys are used for authentication. The authors in [14] have proposed two token based approaches named Magkey, and Mickey. The Magkey token encodes the authenticating code in a form of a magnetic field that can be

Table 2. 3: OOK bit encoding

Bit	Symbol
0	OFF
1	ON

detected by the smartphone's compass, and the Mickey employs a sound emitter to achieve same encoding that can be detected by the smartphone's microphone. Although both these approaches leverage common smartphone sensors, they suffer from an inherent drawback in terms of sensor reliability. As a compass is embedded deep inside the smartphone, it is practically impossible to filter out stray magnetic fields in the environment whether from the Earth's magnetic field or any electronic devices, or conduction wires that generate a magnetic field that is fluctuating in nature. The same applies to the microphone as it catches the acoustic noise in the environment. On the other hand the natural exposure of a light sensor and a straight light emission on the surface of a smartphone provide an effective isolation of noise especially by employing a physical guard around the light emitter in the FIRE token.

Keeping pace with the evolving shift to use smartphones as primary gateways to the web and cloud services are the newer threat models that are targeted specifically towards smartphones. Threat models as designed in [35] rely on accelerometer, and gyroscope sensors of a smartphone to predict the passwords being typed by the users. The lack of any moderation on use of accelerometer, and gyroscope sensors increases the security risk. Using the FIRE token to authenticate users will defeat such security threats.

Table 2. 4: LIM bit encoding

Bits	First Symbol (lux)	Second Symbol (lux)
0000	10	320
0001	10	640
0010	10	1280
0011	10	2600
0100	10	10240
0101	320	640
0110	320	1280
0111	320	2600
1000	320	10240
1001	640	1280
1010	640	2600
1011	640	10240
1100	1280	2600
1101	1280	10240
1110	2600	10240
1111	10240	10

OptAuth is one of the token-sensor authentication methods that leverages a prevalent sensor in smartphones. It provides the user fast authentication using an inexpensive light-emitting token. We have found that it is highly reliable in that smartphone sensors accurately read the high rate light pulses with little error. It enables the users in rugged conditions and with physical challenges to do authentication.

2.4 Conclusion

We have presented an optical wireless authentication for smartphones, OptAuth that is Fast, Inexpensive, Reliable, and Easy-to-use (FIRE). OptAuth leverages a smartphone's ambient light sensor and uses a challenge-based programmable light-emitting token generator. We have designed and prototyped an inexpensive passcode encoder and light-emitting hardware. Our experiments validated that FIRE token can authenticate a user on

a smartphone in an easy, fast, and reliable way without compromising the security quality. The proposed authentication can be used not only to act as a fast and easy-to-use alternative for emergent or challenging usage scenarios, but also as part of a multi-factor authentication scheme that is fast, inexpensive, reliable, and easy-to-use.

CHAPTER 3

SMARTPHONE BASED CAR2X-COMMUNICATION WITH WIFI BEACON STUFFING FOR VULNARABLE ROAD USER SAFETY

As smart devices gain their popularity, vulnerable road users (VRUs) are increasingly distracted by the activities with the devices such as listening to music, watching videos, texting or making calls while walking or bicycling on the road. They are more at risk of getting involved in accidents with vehicles on the streets [36]. For example, a recent report [36] says “The number of headphone-wearing pedestrians seriously injured or killed near roadways and railways has tripled since 2004” and “In roughly one-third of the cases, horns or sirens sounded before the victim was hit, according to eyewitness reports.” Although various VRU safety infrastructures such as traffic lights, warning signs, and alert sensors are deployed on the streets to reduce the risk of collisions, all such mechanisms are not capable of providing direct alerts to the distracted VRUs tailored to the specific scenarios. Although much of pedestrian safety in intelligent systems is directed towards alerting driver of the vehicle with the pedestrian detection sensors and night time infrared cameras, a direct alert from vehicles to VRUs still heavily relies on the traditional sound warning method. However, the more VRUs are shutting out the external safety related warning sounds especially due to their smart devices. Thus, it is critical to design a bi-directional communication system between vehicles and smart devices of VRUs that can directly exchange personalized alerts either sides to recommend ways to avoid imminent collisions in a timely manner.

Recently researchers in the automotive industry, as well as academia [37], [38], [39] have proposed Car2Pedestrian communication systems that issue alerts between vehicles and VRUs using smart devices, if a situation of potential collisions arises.

In [37], the researchers use the WiFi Direct feature of Android powered devices to establish an ad-hoc network between the smart devices in the vehicles, and those carried by VRUs. They cite that the communication latency to relay a threat to VRUs is low as it takes around 1 second only for the WiFi Direct [40] association time. However, in practical scenarios, it will greatly limit the coverage distance between the devices. For example, according to GIDAS [41], [39], nearly 90% of all accidents are with the vehicle speeds up to 70 km/h (i.e. 20m/s). However, the system only can cover the speed of less than 25 km/h.

In [39] the researchers find that ad hoc communication at high speeds is not possible with the WLAN chipsets. They propose Car2X communication should be enabled by using dedicated short-range communications (DSRC) [42] also known as 802.11p, and the software modules of smart devices for European Telecommunications Standards Institute's Intelligent Transport Systems, which specifies 5.9 Ghz technology (ETSI ITS G5). However, such an approach would require the vehicle manufactures to provide the 802.11p enabled modules in the vehicles. Similarly, in [38] the researchers use 802.11p modules in the vehicles, and modified smartphones for VRUs to enable Car2X communications. As presented in Table 3.1, the range and mobility that DSRC offers

Table 3. 1: Comparison of various wireless protocols

Protocol	Data Rate	Range	Mobility
DSRC	3-27 Mbps	< 1 Km	> 60 Mph

WiFi (with association)	6-54 Mbps	< 100 m	> 5 Mph
Cellular	< 2 Mbps	< 10 Km	> 60 Mph
Mobile WiMax	1-32 Mbps	< 15 Km	> 60 Mph

cannot be matched by the regular WiFi [43]. DSRC, however, is not ubiquitously available yet on VRUs' smart devices, and only available in some vehicles.

In this chapter, we propose a smartphone based Car2X communication system, named WiFiHonk, which can alert the imminent collisions to both VRUs and Vehicles. WiFiHonk provides the cost effective and practical safety means to the distracted VRUs using the WiFi of smart devices. First, we have identified that the severe mobility constraints of the WiFi are due to its communication association latency. Hence, if we are able to override this connection step between the devices, and still achieve the delivery of intended messages, then the devices can communicate even in high mobility cases. To enable the connectionless communications between devices using WiFi without the association latency, we exploit the possibility of using WiFi Beacon Stuffing [44] in Car2X communication scenarios. The Beacon Stuffing approach embeds the intended messages within the SSID or BSSID field of the WiFi beacon header and is available for the smart devices by operating the WiFi Hotspot [45] or WiFi Direct mode.

These beacons are transmitted every 100 ms, and are passively scanned in WiFi Hotspot/Direct discovery mode. Our practical and simulation experiments indicate that WiFiHonk works well up to 70 mph high speed vehicles, and successfully exchange accurate warnings between VRUs and vehicles. Second, we have designed an efficient

Algorithm 3. 1: TB beacon update

TB Beacon Update

1: At start time obtain fine-grained location from GPS satellites;

2: Extract Current Speed (C_s);

3: Get Travel Direction (T_d);

4: while ElapsedTime (E_t) < DecayTime (D_t) do

5: if C_s changes by ±S Mph then

6: Update Beacon;

7: else if T_d changes by ±D° then

8: Update Beacon;

9: end if

10: end while

collision estimation algorithm that can correlate mobility vectors of VRUs and vehicles in order to avoid unnecessary warnings (not to disturb the VRU's original usage experience) as well as to issue appropriate warnings (in their urgency and intensity). For example, a VRU may receive beacon messages from the multiple vehicles. The algorithm can select messages only from the approaching vehicles. It also decides the warning level according to the proximity and speed of the vehicles.

The rest of this chapter is organized as follows. A detailed explanation of the proposed WiFiHonk system is presented in Section 3.1. The performance evaluations are explained

Algorithm 3. 2: TR collision estimation

TR Collision Estimation

1: At start time obtain fine-grained location from GPS satellites;

2: Estimate TR Vector (TR_{Vec});

3: Activate WiFi radio;

4: Execute thread TR_{Vec} Update();

5: while ElapsedTime (E_t) < DecayTime (D_t) do

6: Scan WiFi Beacons;

7: if new or updated TB scanned then

8: Extract beacon from TB_X;

9: Evaluate TB_X vector (TB_{XVec});

10: if TR_{Vec} and intersect TB_{XVec} then

11: Update CollisionTable with TB_X;

12: else

13: Discard TB_X;

14: end if

15: else

16: for each TB in CollisionTable do

17: if Time to Collision < CriticalTime then

18: Alert User;

19: end if

20: end for

21: end if

22: end while

in Section 3.2. Section 3.3 discusses the existing, state-of-the-art Car2X communication techniques. Finally, we conclude the chapter in Section 3.4.

3.1 WiFiHonk Approach

WiFiHonk consists of a beacon stuffing module, a collision estimation module, a collision table, and an alert module. The technique of embedding meaningful information in the access point (AP) discovery messages is called Beacon Stuffing [44]. It enables us to push meaningful information safety alert without incurring the delay of WiFi AP association which can take a few seconds. As presented in Algorithm 3.1, the beacon stuffing module first collects the location from the GPS positioning (latitude and longitude), the speed from the accelerometer sensor (mph), and the travel direction from the gyroscope sensor (degree 0 $\sim$ 360). The collected information replaces the beacon messages SSID field (32 bytes) as a WiFiHonk Information Packet (WHIP). A WHIP packet starts with a special string C2X followed by latitude, longitude, speed, and direction separated by a space. The WHIP stuffed beacon message can be initiated by both vehicles and VRUs called Threat Broadcaster (TB). The TB broadcasts these beacons every beacon interval (i.e, 100 ms). These beacons can be adaptively stuffed when there is a significant change in the location, device speed and/or direction of travel. The collision estimation module calculates an Estimated Time to Collision (ETC) information by using the received WHIP information.

Algorithm 3. 3: TR_{Vec} Update

TR_{Vec} Update()

1: while ElapsedTime (E_t) < DecayTime (D_t) do

2: if C_s changes by ±S Mph then

3: Update TR_{Vec};

4: else if T_d changes by ±D° then

5: Update TR_{Vec};

6: end if

7: end while

When a smart device encounters a WHIP information (starting with C2X) from the SSID field of the beacon message, it also extracts the source MAC address from the information element. The receiving smart device can obtain a unique identifier, Vehicle ID from the message's MAC address. As shown in Algorithm 3.3, it collects local devices location, speed, and travel direction information to calculate its direction vector. Using the direction vectors calculated from the WHIP information (location, speed and travel direction) and the local information, it generates a logical map to identify its own vector along with the direction vectors for various vehicles obtained through WHIP information. These are called Collision Vectors, and if a device can compute these Collision Vectors to intersect a point in the logical map at the same time, then it means there is a possibility of collision in their future travel paths. If an intersection is found, using the speed and location information, it calculates ETC.

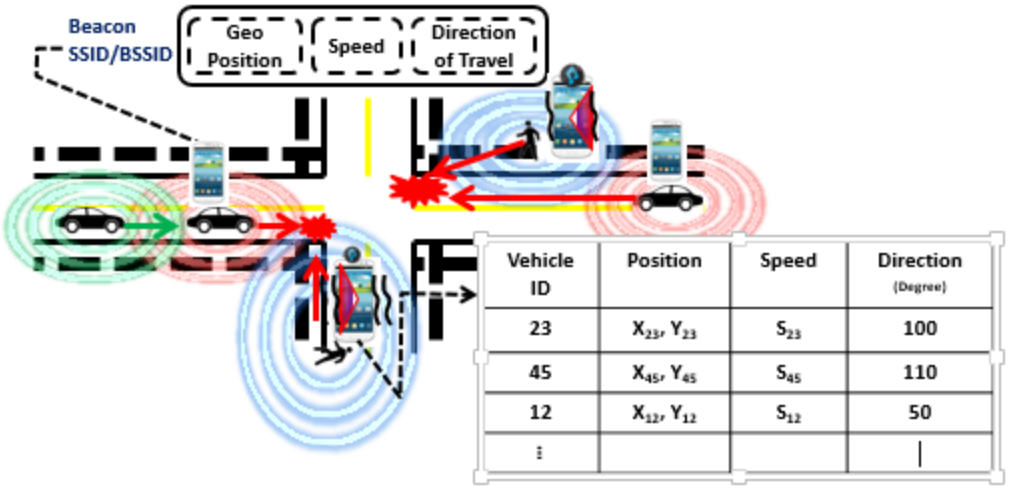


Figure 3. 1: WiFiHonk approach conceptual illustration

When the ETC for a particular entry reaches a configured critical point, an alert module issues an alert via various ways to draw a smart device user's attention such as audio, tactile, and visual alerts via the smart device headphones/speakers, vibrations, and display screen. This operation is called the Threat Receiver (TR), and explained in detail in Algorithm 3.2 and 3.3. The collision table is a database that stores unique vehicle id entries in the increasing order of ToC. The conceptual approach of the proposed WiFiHonk is illustrated in Figure 3.1.

3.2 WiFiHonk Evaluation

We used Samsung Galaxy S3 and Galaxy Tab powered with Android 4.0 to implement WiFiHonk. We experimentally obtain the various environmental factors used in our simulation studies. In practical situations for WiFi Hotspot/Direct, the range for the APs is

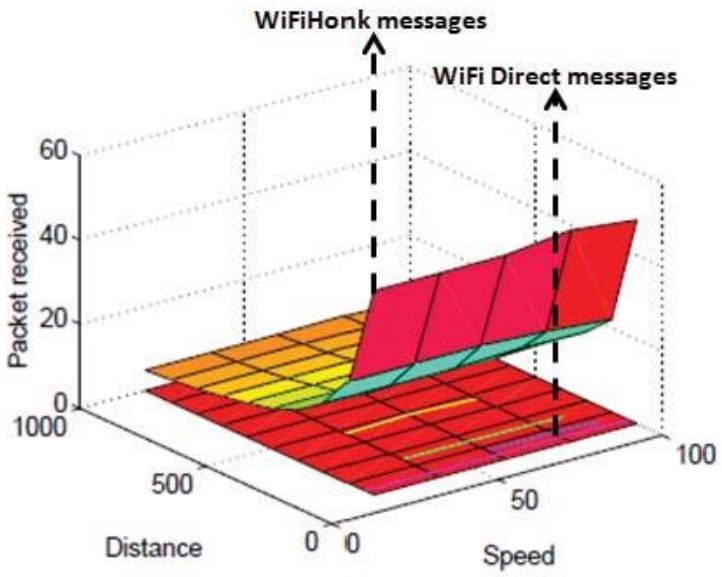


Figure 3. 2: WiFiHonk & WiFi Direct mobility verification: Vehicles crossing each other

~50 m, the association time ~2 seconds, beacon intervals is 100 ms, and time to register an alert for VRU is ~1-2 seconds. We use Rayleigh Fading signal propagation model [46] with environmental noise of 95 db to model losses. The packets lost in a wireless medium are a function of the distance between the transmitter and receiver, and the environmental noise. The average bit error probability PB is calculated using the following equation:

$$P_B = \frac{1}{2 * (1 + SNR)}$$

$$where\ Signal\ To\ Noise\ Ratio\ (SNR) = RSSI + Noise$$

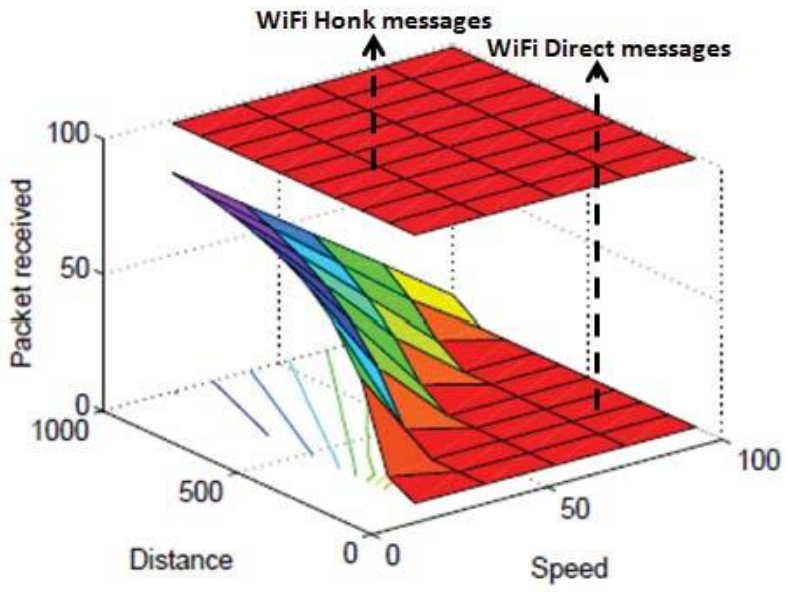


Figure 3. 3: WiFiHonk & WiFi Direct mobility verification: Vehicles following each other

The observed Received Signal Strength Indictor (RSSI) for the smart devices at different distances between transmitter and receiver are shown in Table 3.2. The VRU gait is 3.1 mph, and vehicle speed is varied.

First, we verify if WiFiHonk can successfully deliver at least one beacon in a timely manner for a wide range of speeds and mobility scenarios, as just one beacon containing the WHIP packet is enough to estimate if there will be a collision. We emulated an environment in which two vehicles are crossing each other and following each other for varying speeds and distances. We also compare WiFiHonk's performance with the traditional association based WiFi Direct method for transmitting messages. In both cases, the broadcast interval of the messages was 100 ms. As shown in Figure 3.2 and

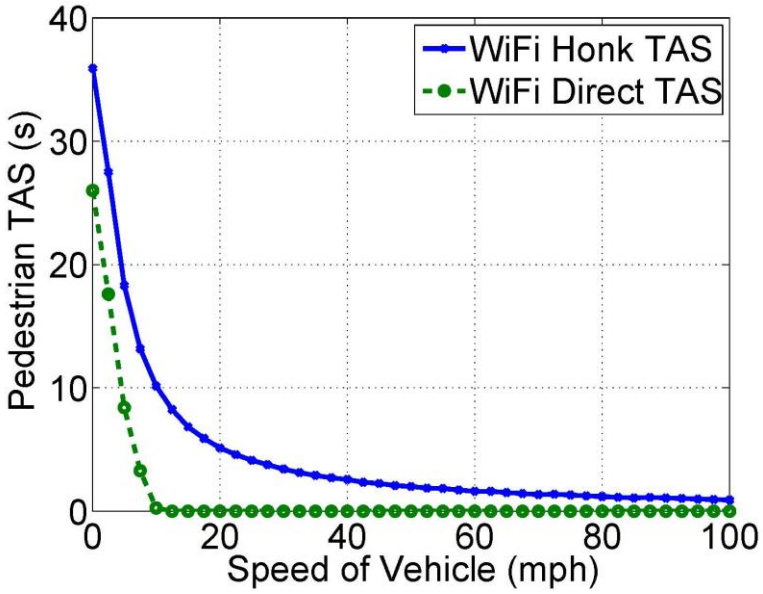


Figure 3. 4: WiFiHonk evaluation - VRU time available to stop

Figure 3.3, WiFiHonk successfully delivers at least one message for both the cases for all settings of mobility speed and distance. It should be noted that WiFi Direct based method fails in delivering even a single message for the case in which the two vehicles are crossing each other when the speed is greater than 15 mph. Vehicles crossing in some format is the most basic setting for most type of collision.

Next, we carried out simulation tests for various crash scenarios, and obtained results determining the Time Available to Stop (TAS) and Probability of Collision (POC) for a VRU after the alert is received using WiFiHonk, and compared it with WiFi Direct method. We used the following formula to compute POC, as it is inversely proportional to TAS combined with the Time necessary by a VRU to recognize the Alert on smart device (TRA).

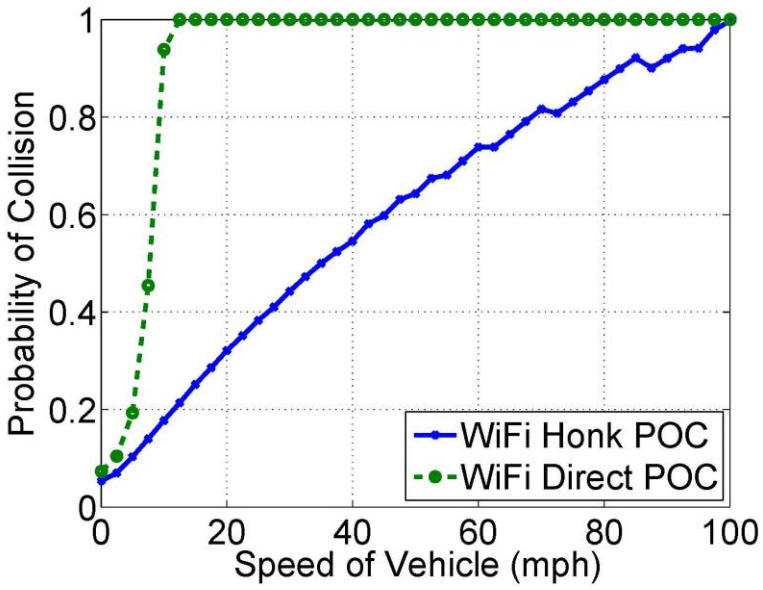


Figure 3. 5: WiFiHonk evaluation - probability of collision

We assume 1 second for the Required Time to Sop (RTS), and 1∼2 random time for TRA in the evaluation. POC becomes 1 if TAS is 0 second.

$$POC = \frac{RTS}{TSA + TRA} \; if \; TSA \neq 0$$

For a crash scenario similar to one in Figure 3.1, Figure 3.4 shows that with WiFiHonk a VRU can be safely alerted of a collision is a timely manner even for high speeds, whereas WiFi Direct based method works well till only ∼10 mph of vehicle speed. In addition, the resultant POC is reduced due to the use of WiFiHonk as shown in Figure 3.5. Based on the POC, we can alert the driver of the vehicle as well as the VRU in a more aggressive mode of WiFiHonk where VRUs' device also acts in AP mode.

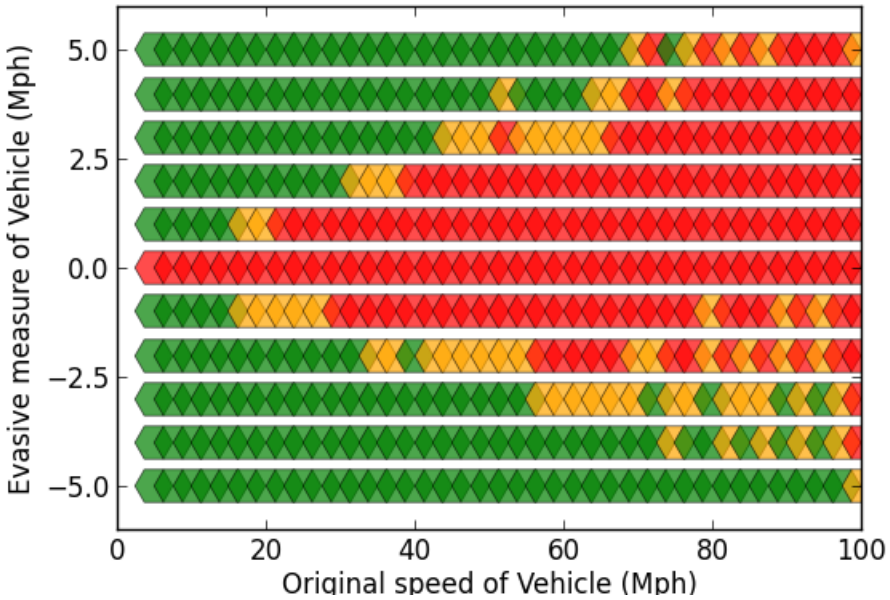


Figure 3. 6: WiFiHonk vehicle evasive measures

Based on the TAS and POC results, we estimate the outcome of the situation for various conditions of braking or accelerating to avoid the accident as shown in Figure 3.6, and Figure 3.7. While Figure 3.6 shows the outcome of the scenario when a vehicle responds to the WiFiHonk alerts by accelerating or decelerating to avoid hitting the VRU, Figure 3.7 shows the outcome when similar evasive maneuvers are made by the VRU. Green zone indicates successful evasion of accident, orange zone indicate high risks, and red zone indicate definite collisions. In the green zone, a driver and a VRU(s) can be alerted with recommendations to avoid an accident in a timely manner. We observe that WiFiHonk alerts are important to be delivered to the smart device in a vehicle, as evasive measures by the vehicle result in better outcomes where crashes are avoided. As for a

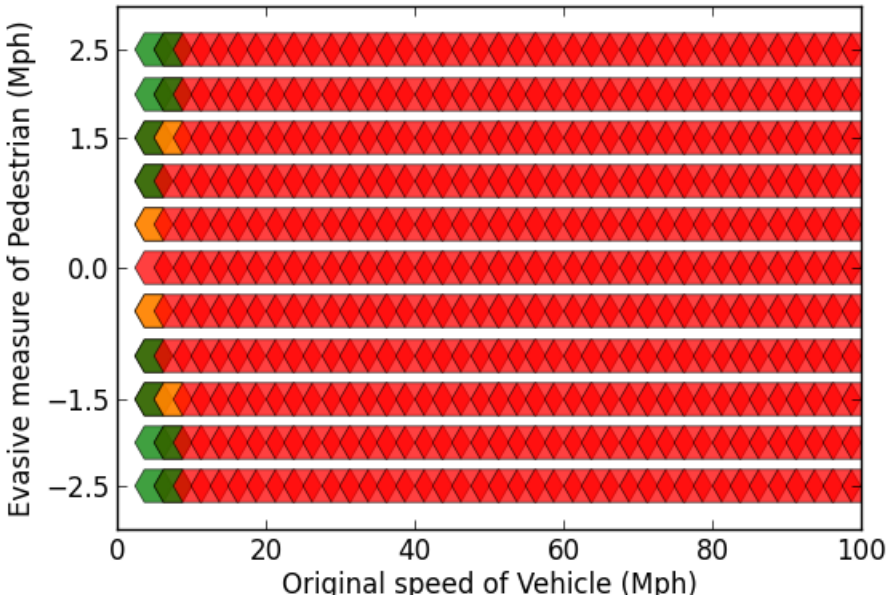


Figure 3. 7: WiFiHonk pedestrian evasive measures

VRU, the crash can be avoided mostly only if they completely stop moving, and attempting to run or slow down the pace are not effective in avoiding the accident. It should be noted that 90% vehicle-VRU accidents occur at 43.5 mph [39]. WiFiHonk will successfully avert such accidents unlike existing approaches.

3.3 Related Work

Various Car2X safety application can be identified in literature that use different communication mechanisms including GSM/CDMA networks, DSRC based communication, and adhoc WiFi based communication in smart devices.

GSM/CDMA communication based techniques [47], [48], [49], [50] rely on the smart devices onboard the vehicle to detect, and relay accident information using the sensors on the smart phones. They use the GSM/CDMA connectivity to make the other vehicles, and emergency responders aware of the accident. They aim to improve the driving conditions, and response time of the emergency responders in getting to the accident site. Such GSM/CDMA techniques are not suitable for accident prevention due to the high latency incurred due to interaction with third party servers that are used to relay the messages between devices.

DSRC based techniques [38], [39] aim to use a DSRC onboard unit for special vehicles to detect the presence of VRUs on the streets using their smart device to alert the driver in case of collisions. The smart devices are equipped with ETSI ITS G5 software modules to enable the interaction with the DSRC unit aboard the vehicles. While such DSRC based techniques satisfy the low latency requirements of accident prevention applications, they require expensive additional DSRC equipment that vehicle manufacturers should fit their vehicles with. In addition, it presents a challenge to older or regular models of vehicles with no DSRC unit.

Ad-hoc WiFi connection techniques use the WiFi Direct feature in Android powered devices to enable P2P communication between them [37]. However, the additional delay introduced by the connection setup process of the WiFi consumes precious time. This results in degraded performance of such systems when the vehicle is traveling at speeds upward of 15 mph as demonstrated in our results.

Table 3. 2: Emperical average of measured RSSI for various distances

Distance between devices (m)	10	20	30	40	50
Measured average RSSI (dB)	-70	-75	-80	-85	-90

Some standalone applications that use the camera and other sensors to detect presence of vehicles, and estimate the threat of collision have also been proposed [51]. However, such techniques will require the user to position the camera appropriately capturing the street while walking. It should be noted that not only will it be difficult for VRUs to ensure that while walking, but also that the camera does not capture 360 degree view of the environment unlike the radio frequency techniques that are omnidirectional in nature. For example, if the camera of a VRU in is pointing ahead, such technique will not be able to avert a collision with vehicle approaching from behind.

WiFiHonk on the other hand uses the beacon stuffed WiFi messages to overcome the mobility challenges imposed by the connection oriented WiFi approach. Our experiments and simulation studies have found that WiFiHonk can alert VRUs of possible collisions successfully for high speeds, and various collision scenarios.

3.4 Conclusions

We have proposed an active VRU safety mechanism called WiFiHonk that uses Beacon Stuffing to alert VRUs of collision with vehicles using smart devices. We demonstrate the efficacy of WiFiHonk in successfully alerting the VRUs of collisions even for very high speeds which is not possible with the approaches currently available.

CHAPTER 4

ENERGY-EFFICIENT COOPERATIVE OPPORTUNISTIC POSITIONING FOR HETEROGENEOUS SMART DEVICES

Smart mobile devices such as smartphones and tablets are rapidly becoming prevalent in our lives. They have spurred a paradigm shift from traditional restricted phone applications to intelligent mobile applications such as location-based, context-aware, and situation-aware services. For example, a social-network-based traffic information system [52] allows each mobile user to report and use real-time traffic information, in addition to the archived traffic information from the US Department of Transportation.

As many of those application services require position information, smart mobile devices provide various positioning services via Global Positioning System (GPS) [53], WiFibased positioning system (WPS) [54], or Cell-ID Positioning [55]. Being dedicated equipment for positioning, GPS becomes available for many smart devices as an additional feature and is considered to be an accurate and preferred method for location-based services (LBSs) [56], [57]. However, its high energy consumption, due to the Time To First Fix (TTFF), becomes a significant drawback. WPS approximates a position from the location information of a nearby wireless access point (AP) that is stored in the database. Its energy efficiency is much better than GPS, and the accuracy is moderate.

Table 4. 1: Characterization of various positioning methods

Positioning Method	Accuracy	Energy Efficiency	Equipment Availability	Service Limitations
GPS	High (~ 10 m)	Low	Low	Indoor & canyons
WPS	Medium (~ 50 m)	Medium	High	Coarse AP density areas
Cell-ID Positioning	Low (~ 5 Km)	High	Medium	Rural areas

As WiFi is a de facto standard in wireless local area network (WLAN) communication, it is broadly available on most smart devices. However, the service is limited to indoor or urban areas where the access points are densely populated. Cell-ID Positioning provides an approximate location from the serving cell tower, where a cell area range is around 100 ∼500 m in urban areas, but it can span up to 10 Km for rural areas. Although this is the most power saving approach, due to a large error range caused by the coarse cell tower density, Cell-ID Positioning cannot offer the utility of most LBS applications. In addition, mobile devices such as the WiFi version of tablets are not fully equipped with 3G/4G data chips at the present time even though 3G and 4G wireless networks provide enough bandwidth to enable explicit support for real-time LBS. We have summarized the characteristics of positioning methods ([58]) in Table 4.1.

Energy efficiency while maintaining required accuracy for the given service limitations is one of the most critical issues in mobile devices, due to limited battery life and the high energy consumption of applications. As different positioning methods available on a mobile device have different characteristics with respect to accuracy, energy-efficiency, and service availability, there have been several proposals for dynamic selection of a

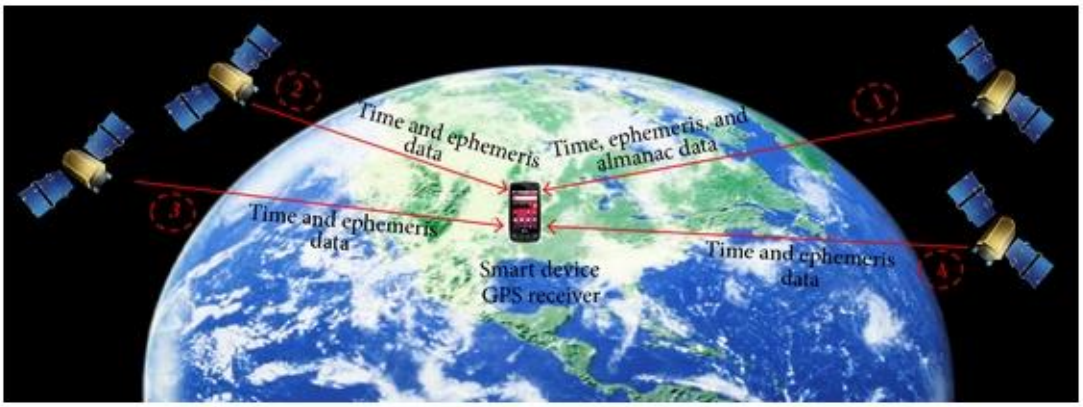


Figure 4. 1: Illustration of global positioning system

positioning method on an individual device. For example, [59] uses an accelerometer for movement detection to power cycle GPS, if the device is not mobile. However, the effectiveness of most of the existing heuristics is limited by equipment constraints or service availability, as the applications choose a preferred positioning method that is available within an individual device.

In this chapter, we propose ECOPS to facilitate a WiFi hotspotmode [60] or WiFiDirectmode [61] based approximation in collaboration with a few available GPS broadcasting devices under budget constraints. ECOPS is a collaborative positioning method between WiFi and GPS mobile devices, in addition to a positioning method selection heuristic within a mobile device. It can achieve moderate accuracy with low energy usage. Although there is a previous collaborative work [59] that pairs two devices via Bluetooth to save GPS power cycle, the approach needs both GPS and Bluetooth on

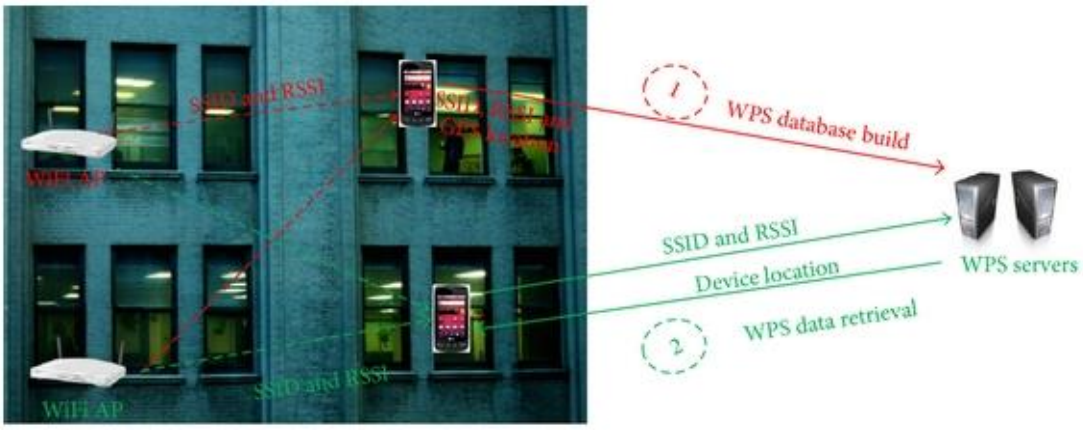


Figure 4. 2: Illustration of WiFi positioning system

both devices. Instead, ECOPS supports heterogeneous methods among mobile devices. There are many mobile devices including the majority of current tablets that only support a basic wireless communication method which is WiFi. The WiFi-only device can obtain position information from a GPS device with ECOPS. This proposed system can operate opportunistically, where each device can resolve the location via various available methods including trilateration [62] with three GPS broadcasting devices and a received signal strength indicator (RSSI) [63] or approximation with geomagnetic sensors [64] and a single GPS device without requiring any WiFi AP.

We implemented ECOPS using Android-powered mobile devices such as smartphones and tablets. The evaluation results show that ECOPS significantly saves the total energy consumption of the devices while achieving a good level of location accuracy. In addition,

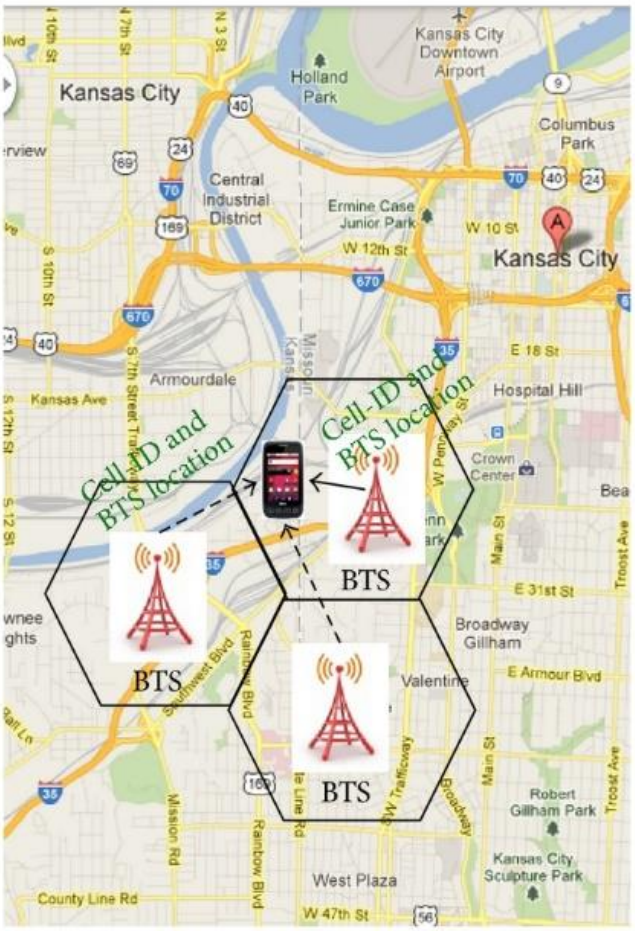


Figure 4. 3: Illustration of Cell-ID positioning

it enables constrained devices to enjoy location-based services that would otherwise not be possible.

The rest of the chapter is organized as follows. Potential application scenarios are described in Section 4.1. Section 4.2 discusses the existing and state-of-the-art techniques. A detailed explanation of the proposed system is presented in Section 4.3.

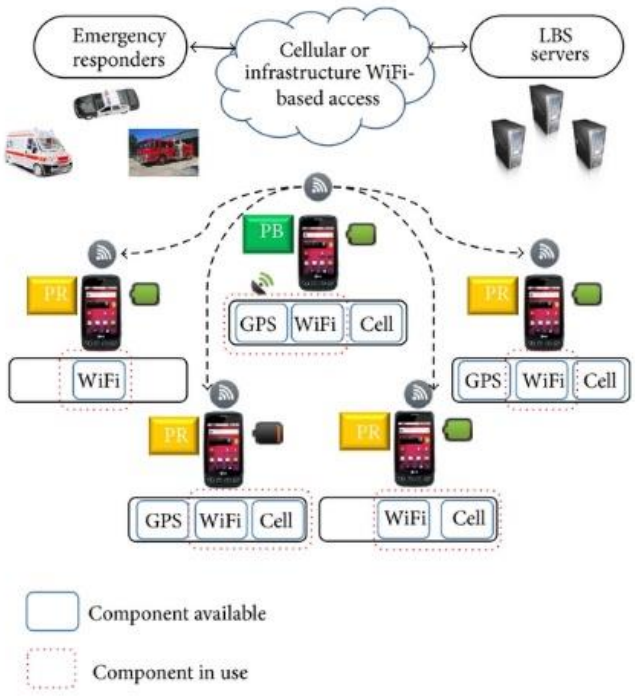


Figure 4. 4: ECOPS deployment example

The performance evaluations and experimental scenarios are explained in Section 4.4. Finally, we conclude the chapter in Section 4.5.

4.1 ECOPS Application Scenarios

While security and social incentive issues are not in the scope of this paper, the proposed opportunistic and collaborative positioning scheme can be especially useful for unique resource scarce and mission critical applications. Such examples include border patrol, battlefields, mountaineering expeditions, and disaster area assistance.

For example, suppose a team of border patrol officers is searching for an illegal immigrant in the border area. In some areas of rigid terrain, GPS and cellular signals can

Algorithm 4. 1: ECOPS: Initial procedure deciding whether a device becomes either a PB or a PR

Main()

1: check the residual power (p_r);

2: if GPS-equipped device & $p_r \geq p_{min}$ then

3: device becomes PB and activatesWiFi hotspot;

4: executes CollaborativePB();

5: else if non-GPS device || $p_r < p_{min}$ then

6: device becomes PR and executes CollaborativePR();

7: end if

be lost in a canyon. Some projects [65] employ a low-altitude tethered aerostat to set up a temporary WiFi hotspot. To help with positioning, a few officers stay at the top of the valley to relay their GPS position information to the officers searching down in the valley. Such a collaborative positioning is a natural application scenario of ECOPS.

In a battlefield scenario, when a platoon is air-dropped into a war zone, it is nearly impossible to find WPS services in the surroundings. Even with the availability of technology like LANdroids [66] to provide a network in such conditions, it is not a simple task. Also, it is crucial for soldiers to have accurate location information in the battlefield. In such a scenario, the capabilities of ECOPS can be exploited to maintain accurate location information while reducing overall energy consumption. Although one may not have a strong incentive to take a lead and offer location information for others, such

Algorithm 4. 2: ECOPS: CollaborativePB()

CollaborativePB()

1: while $p_r \geq p_{min}$ do

2: listen to connection request from a PR;

3: wait for location request from a PR;

4: if PR requests then

5: check the time elapsed since the device got location information (t_e)

6: calculate I_{decay};

7: if $I_{decay} < \alpha$ then

8: update its GPS location information;

9: $t_e = 0$;

10: end if

11: end if

12: broadcast current GPS location information;

13: check the residual power (p_r);

14: end while

15: execute CollaborativePR();

concerns are lifted immediately if a leadership hierarchy preexists in the application scenario. For instance, when a platoon is being deployed in a battlefield, the platoon leader chooses to be the primary location broadcaster using ECOPS along with a few others at the top of the hierarchy. The other soldiers in the unit are able to estimate their

Algorithm 4. 3: ECOPS: CollaborativePR()

CollaborativePR()

1: while non-GPS device || (GPS-equipped device & $p_r < p_{min}$) do

2: sleep until the device needs to update location information

3: numofPBs = 0;

4: check the list of available PBs;

5: make connection to each PB and request GPS location information sequentially;

6: calculate the distance to each PB using the obtained RSSI value;

7: set numofPBs to the number of the detected PBs

8: if numofPBs == 1|| one of PBs is within the near field threshold (β meters) then

9: use the received GPS location information immediately without trilateration;

10: continue;

11: end if

12: if numofPBs == 2 then

13: calculate two possible locations (PR) and get the middle location between the two possible locations;

14: end if

15: if numofPBs >= 3then

16: select three PBs randomly and calculate the its current location (PR) with the GPS coordinates and distance information of the selected PBs;

17: end if

18: if GPS-equipped device then

19: check the residual power (pr);

20: end if

21: end while

22: execute CollaborativePB();

location information based on the geo-coordinates they receive from their unit's command. This will result in fewer devices from the unit querying satellites for location information and reduce the overall energy consumption. Extending the lifetime of devices during the operation is a mission critical parameter as the duration of an operation is not fixed and often tends to be longer than expected. Under the Battlefield Air Targeting Man Aided Knowledge (BATMAN) [67] project, the United States Air Force is actively seeking to equip their soldiers with modern Android-powered smartphones to obtain accurate location information with high energy efficiency. Modified versions of Android [68], [69] enable the desired level of security for military use. Such projects can benefit greatly by ECOPS.

Another scenario where ECOPS can be extremely useful is during natural calamities. In such cases, emergency responders who are involved in search and rescue missions can host an ECOPS-based location broadcasting service over WiFi Direct. As they move around the area, victims can use their smart devices to either request assistance or transmit their locations.

4.2 Related Work

Positioning schemes on mobile devices have been a long standing topic of exploration. This resulted in three main positioning techniques using either the information provided by the GPS, WPS, or Cell-ID Positioning. Also, there have been several research proposals for specific environments.

The Global Positioning System (GPS) is a satellite navigation system that provides location and time information anywhere on earth with four or more GPS satellite signals. It is originally deployed and maintained by the United States government and is now freely accessible to anyone [53]. The GPS provides very high level of accuracy, but suffers from a high TTFF due to the large distance between the GPS receiver and serving satellites. This problem has been somewhat addressed by the use of assisted GPS (aGPS) that relies on the cellular or internet infrastructure to get a faster lock on the serving satellites while obtaining precise time information from the network.

Within the navigation message continuously broadcasted by each of the satellites in the constellation, the GPS receiver looks for three important pieces of data as illustrated in Figure 4.1. The first piece of data consists of the GPS date and time information. It additionally also consists of the health statistics of the satellite. The ephemeris data forms the second important piece and allows the GPS receiver to calculate the position of the satellite and is broadcasted every 30 seconds. The ephemeris data is valid for no longer than four hours. The third important piece is the almanac data which provides approximate information concerning the rest of the satellites. This data is transmitted over 12.5 minutes and is valid for a maximum of 180 days. The almanac data can be obtained from any satellite, and it enables the GPS receiver to determine which particular

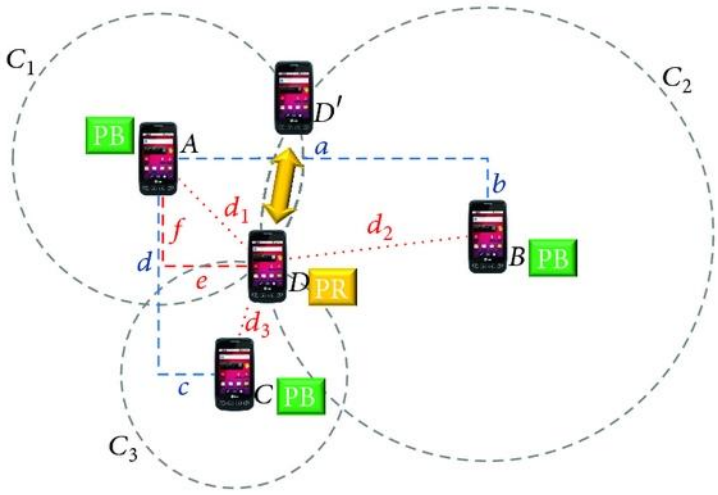


Figure 4. 5: 2D trilateration

satellite to search for next. As the signal from the selected satellite becomes directly available, the GPS receiver then downloads the second important data, that is, the ephemeris data. It is absolutely necessary that the GPS receiver has the satellite's complete copy of the ephemeris data to determine its position. In case the signal is lost in the middle of acquiring this data, the GPS receiver will have to discard whatever data was downloaded and start searching for a new satellite signal.

Once the GPS receiver has ephemeris data directly from three or more satellites, it can carry out various methods to accurately determine its own location. These methods involve and are not restricted to 3D trilateration, Bancroft's method, and multidimensional Newton-Raphson calculations. Due to the high propagation delays, getting the ephemeris and almanac data can take up to 15 minutes for a device just out

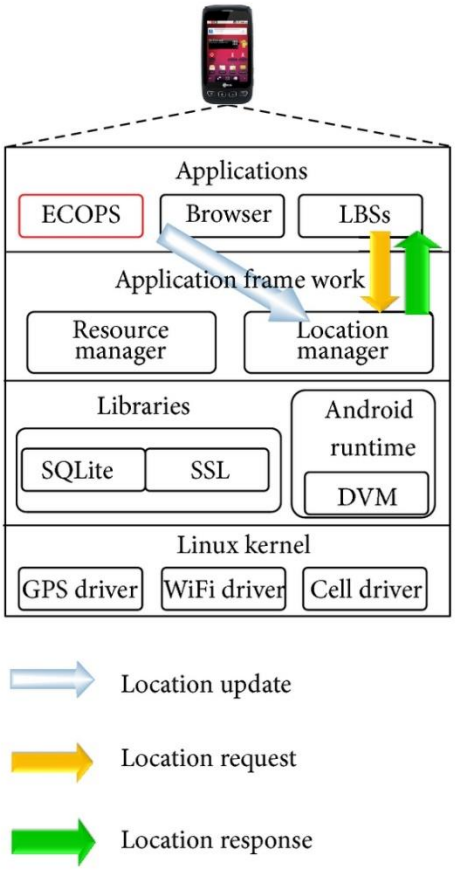


Figure 4. 6: Android module architecture

of the factory, and then around ~20 seconds after the initial configuration. To expedite this process, some GPS receivers can use multiple channels for faster fixes. Another strategy is to obtain the ephemeris and almanac data from a faster network like the cellular network or the internet as in the case of a GPS.

The WiFi-Based Positioning System (WPS) maintains an extensive database of WiFi access points (APs) along with their geographic locations [70], [71].This information has

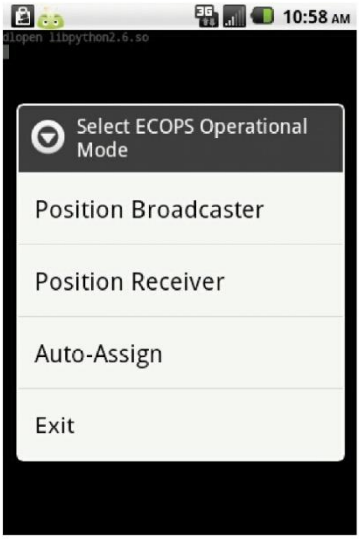


Figure 4. 7: ECOPS screenshot

to be collected painstakingly over a large duration of time and is vulnerable to changes in the location of APs or the discontinuation of their service. The information of AP's SSID and geographic location can be collected manually or in amore automated way by retrieving the GPS location of smart devices connected to the AP and associating that information with the AP. Once such a large and dedicated database is ready and a device is in the vicinity of an AP, or several APs, it can provide the RSSI values and the SSID of the APs to the WPS servers. The WPS servers, based on proprietary techniques, apply filtering approaches and trilateration techniques to this data and determine the accurate location of the smart device. This geographic location information is then relayed back to the smart device which can exploit it for various LBSs. The illustration of WPS is depicted in Figure 4.2.

While the WPS service approaches work well in terms of energy efficiency [72], [73], [74], they are not globally available for users. A solution leveraging the existing infrastructure, such as APs without requiring any specialized infrastructures for localization, has been proposed in [75]. However, since this localization scheme is limited to the indoors and still relies on infrastructure, such as APs, it cannot be useful outdoors where the WiFi signals are neither dense enough nor covered.

In Cell-ID Positioning, a mobile device obtains its position from the geographic location of its associated base transreceiver station (BTS), with an error range proportional to the signal strength within a cell. The mobile device can estimate its location as the BTS periodically broadcasts its Cell-ID along with its location. Once this information is available to the mobile device, it can use the location of the BTS as its own location with the error calculated using the propagation model. Another technique that may be used for cell phones to estimate their location is to observe the delay in receiving a special message broadcasted by the BTS from the time it was transmitted. This information is used by the mobile device to estimate its distance from the BTS.

Note that a cell size can be very large especially in rural areas and highways where the density of cellular towers is very low. One cellular tower is often capable for serving up to 5 Km radius. As this large cell size leads to a significant error range, other nearby cell tower signals may be used in order to improve the accuracy [55, 76]. Such approaches also exploit the fading phenomenon independently or along with predictive techniques to improve the accuracy of Cell-ID Positioning. However, the accuracy is still limited as the propagation model needed for the trilateration does not work well, due to complex signal

fading behavior over long distances. The illustration of Cell-ID Positioning is depicted in Figure 4.3.

In other recent research proposals, while most of commercial approaches heavily depend on infrastructures [54, 77], or use extra high-end sensors and exploit the available information from an individual device [77], [78], [79], research proposals mostly aim to improve the positioning accuracy or energy efficiency through algorithmic approaches [59], [74], [75], [80], [81], [82], [83], [84].

The work in [82], [83], [84] attempt to learn a known location from a training phase for a better location accuracy. The authors of [84] employ indoor positioning, and perform fingerprinting and training of the known space using multiple sensors in a smartphone such as WiFi radio, cellular communications radio, accelerometer, and magnetometer. In order to improve Cell-ID location accuracy in low-end cell phones where neighboring cell tower information is not available, [83] uses RSSI from only the associated cell tower and leverages the signal strength history to estimate the location. The Cell-ID Aided Positioning System (CAPS) [82] relies on the continuous mobility and position history of a user to obtain better location accuracy over a basic cell tower-based approach. It uses Cell-ID sequence matching to estimate current position based on the history of Cell-ID and GPS position sequences that match the current Cell-ID sequence. CAPS assumes that the user moves on the same routes repeatedly and has the same cellular chip and infrastructure availability.

A few studies address energy efficiency of smartphones using power duty cycling techniques [58], [59], [82] that use a combination of the basic positioning techniques in a smartphone.

The authors of [58] use different positioning schemes depending on the condition, for the purpose of target tracking. In the scheme, energy-efficient but inaccurate Cell-ID Positioning or WPS is used when the target is distant, while accurate but energy-inefficient GPS is used when the target is close.

The rate-adaptive positioning system (RAPS) [59] uses built-in sensors in a smartphone to determine if the phone has moved beyond a certain threshold and decides whether to turn on the GPS or not. RAPS also stores the space-time history of the user's movements to estimate how to yield high energy efficiency. Another idea presented by the authors involves a Bluetooth-based position synchronization (BPS) in which devices share their location information over a Bluetooth connection. While a Bluetooth connection consumes less power as compared to a WiFi ad hoc, it also limits the range of communication to less than 10 m. Our work has advantages over the basic BPS technique in several aspects. Not only does a WiFi ad-hoc mode give us a better range, but we have also taken into account the heterogeneity amongst the devices in terms of availability of a GPS chip or cellular connection. We expect all the devices to have at least a WiFi module present onboard. In BPS, once location information is obtained from a neighboring device, only a fixed error range of 10m (e.g., same as the range of a typical Bluetooth) is associated with that information. However, in ECOPS we exploit the RSSI values of the connection to determine the accurate distance between the two devices, and when three

or more location transmitting devices are available, the trilateration technique achieves pinpoint locating capabilities.

The work in [85] proposed to use minimal auxiliary sound hardware for acoustic ranging in order to improve the accuracy. The acoustic ranging technique estimates the distance among peer phones, then maps their locations jointly against a WiFi signature map subject to ranging constraints. It is a WPS augmentation technique to improve the accuracy over a pure WPS.

Our approach is unique in that we use a collaborative approach rather than focusing on the information in an individual device and do not rely on any special hardware or infrastructure such as WPS or Cell-ID Positioning. Note that we only use a small amount of GPS information and the WiFi ad-hoc mode of mobile nodes. ECOPS is specifically aimed at resource constrained environments such as battlefields where GPS is the only available positioning infrastructure, and WiFi ad hoc mode is readily available in most mobile devices while allowing good network range (up to 100m). Besides controlling energy usage and the location accuracy, we allow to use heterogeneous mobile device types.

4.3 ECOPS Approach

In this section, we discuss ECOPS algorithms in detail. Figure 4.4 shows an ECOPS deployment example. It consists of mobile devices with heterogeneous positioning methods available such as GPS, WiFi, and Cell-ID. These devices virtually establish an ad hoc network using WiFi to build a collaborative positioning environment. In the

established ECOPS ad hoc network, a device may function as either a position broadcaster (PB) or a position receiver (PR). A GPS equipped device with sufficient battery life and up-to-date location information becomes a candidate for a PB. Other devices with no GPS that need current location information will become PRs.

Three algorithms are presented for the overall operation of the ECOPS. Algorithm 4.1 describes the initial procedure deciding whether a device becomes a PB or a PR. After the initial decision, Algorithms 4.2 and 4.3 depict how the devices in ECOPS collaboratively maintain their most updated location information as a PB or a PR, respectively. For GPS-equipped devices, the role of the devices can be changed during their operation according to their residual energy level (i.e., PB $\leftrightarrow$ PR). As illustrated in Algorithm 4.1, a device, once it starts ECOPS operation, will check the time elapsed since the device got the location information (t_e) and residual power (p_r) to see if it is qualified for being a PB. Since we are looking for the devices that have the most recent location information with enough residual power, the device with the conditions such as $p_r \geq p_{min}$ and $I_{decay} \geq \alpha$ can be a PB, where p_{min} is the minimum residual energy that a PB has to maintain and I_{decay} is the level of the validity with respect to time for the location information, defined by the following equation:

$$I_{deacy} = 100 * (1 - \frac{t_e}{t_d})$$

where t_d is the maximum time in which the location information is considered to be valid.

If a device is equipped with a GPS receiver and satisfies the p_{min}, it can be a PB. Once it becomes a PB, it will start its WiFi hotspot mode and serve the most up-to-date location

information to a PR when a PR requests the location information. An Android device cannot use the WiFi Internet service while it is in the WiFi hotspot mode. However, with (Android 4.0), WiFi Direct technology can be used for PBs. In a PB mode with WiFi Direct, the users can enjoy their WiFi Internet service and provide the most up-to-date location information simultaneously. The device without a GPS receiver will automatically be a PR once it enters ECOPS, and then search for PBs around it.

As shown in Algorithm 4.2, once the device enters the PB mode, it plays a role of the PB while it satisfies the p_{min} constraint. The threshold α is a system parameter that can be varied according to the requirement of applications. The tradeoff between location accuracy and energy consumption can be adjustable using α. An application requiring high accuracy will select a small amount of α, but a high value of α is used for applications requiring low energy consumption. The PB will check I_{decay} to see if the current location information is adequate (e.g., $I_{decay} \geq \alpha$) before broadcasting it.

In Algorithm 4.3, a PR will collect the possible number of GPS coordinates and corresponding RSSI values and apply opportunistic localization as illustrated in Figure 4.5. If a PR finds a PB within the threshold distance (β meters), then a PR uses the GPS coordinate from a PB as is. The parameter β is controllable and users of ECOPS can set it according to their preference. Once a PR estimates its location, it can become a PB. However, we do not use those cases in our experiments to avoid the additional errors that will be induced from PBs and focus on the PR's accuracy.

ECOPS is opportunistic, meaning that getting the most updated location via trilateration is not limited by the number of available PBs. Supposing that there is only one GPS broadcaster in Figure 4.5, say node C, then the center of an error range of the circle C_3 will become the PR's approximated position. Another possible situation is when there are two PBs, say nodes A and B; then the middle point of two possible points, D and D', is selected as an approximated PR location. The accuracy of the estimated location will range from one point where the two circles intersect in the best case to the diameter of the smaller circle in the worst case, respectively. In order to get the most accurate location information for a PR, we need at least three PBs to provide their location information obtained from the GPS receiver along with the RSSI values, so that we can build an absolute coordinate system from the relative coordinate system. For example, in Figure 4.5, we calculate the distance parameters a, b, c, and d using the algorithm described in [86] in order to obtain the values of e and f.We convert the obtained distances e and f into the unit of the GPS coordinates to get the final calculated GPS coordinate. The distance between two GPS coordinates, (lat_1, lng_1) of e and (lat_2, lng_2) of f, is computed using the haversine formula that gives a spherical distance between two points from their longitudes and latitudes [86, 87]. The formula is described in the following equation:

$$F_{dist}(lat_1, lng_1, lat_2, lng_2) = rad\ 2\deg(a\ cos(dist)) * 60 * 1.1515 * 1.609344$$

and and the formula for the value of dist is shown in the following equation:

$$dist = \sin(\deg 2\, rad(lat_1)) * \sin(\deg 2\, rad(lat_2)) + \cos(\deg 2\, rad(lat_1)) * \cos(\deg 2\, rad(lat_2)) * \cos(\deg 2\, rad(lng_1 - lng_2))$$

Thus, we can calculate relative coordinates (a, b, c, and d) with the following equations:

$$a = F_{dist}(A_{lat}, A_{lng}, B_{lat}, A_{lng})$$

$$b = F_{dist}(A_{lat}, A_{lng}, A_{lat}, B_{lng})$$

$$c = F_{dist}(A_{lat}, A_{lng}, C_{lat}, A_{lng})$$

$$d = F_{dist}(A_{lat}, A_{lng}, A_{lat}, C_{lng})$$

The distances (d_1, d_2, and d_3) between node D and other nodes (A, B, and C) can be derived from the measured RSSI values of node D, using the following formula from the path loss propagation model [37]:

$$RSSI = -(10n * \log_{10} d) + \delta$$

where RSSI is the received power which is a function of the distance between the transmitter and the receiver (T-R), n is the signal propagation constant (also called propagation exponent), d is the T-R separation distance in meters, and δ is the system loss factor. Based on the previous equation, we derived the distance (d) between two devices using the average RSSI value with the following equation:

$$d = 10^{(-RSSI - \delta)/10n}$$

Now, the three circles in Figure 4.5 can be represented by the following three equations, respectively:

$$C_1 : X^2 + Y^2 = d_1^2$$

$$C_2 : (X - a)^2 + (Y - b)^2 = d_2^2$$

$$C_3 : (X - c)^2 + (Y - d)^2 = d_3^2$$

where the location of node A is set to (0, 0).

We obtain the relative coordinate of PR node D from node A, (e, f), by calculating the point where these three circles intersect. In other words, we want to calculate the coordinate values of X and Y that simultaneously satisfy the equations for C_1, C_2 and C_3. We first extend the equations for C_2 and C_3 as follows:

$$C_2 : X^2 - 2aX + a^2 + Y^2 - 2bY + b^2 = d_2^2$$

$$C_3 : X^2 - 2cX + c^2 + Y^2 - 2dY + d^2 = d_3^2$$

By applying the equation for C_1, the equations for C_2 and C_3 can be rewritten as:

$$C_2 : d_1^2 - 2aX + a^2 - 2bY + b^2 = d_2^2$$

$$C_3 : d_1^2 - 2cX + c^2 - 2dY + d^2 = d_3^2$$

Finally, the node D's coordinate that satisfies the three circles is attained by replacing X and Y with e and f, respectively, in the previous equation. We can formulate the equations in terms of e and f as follows:

$$e = \frac{d(D_{vec1}) - b(D_{vec2})}{2(bc - ad)}$$

$$f = \frac{c(D_{vec1}) - a(D_{vec2})}{2(ad - bc)}$$

where

$$D_{vec1} = d_2^2 - d_1^2 - a^2 - b^2$$

$$D_{vec2} = d_3^2 - d_1^2 - c^2 - d^2$$

We have implemented ECOPS as an Android application for a feasibility test and analysis. Figure 4.7 shows the screenshots of the ECOPS application. Figure 4.7(a) displays the main screen that allows users to manually select an ECOPS device option either in PB mode or PR mode, or to request the selection automatically based on various parameters such as the remaining energy and sensor availabilities. Figure 4.7(b) presents a PB screen that lists the broadcasting location information. Figure 4.7(c) shows a PR screen that lists the received information and measured distance using the RSSI value. Although the current implementation is on an application level, as illustrated in Figure 4.6, it is still capable of making the received location information available to other application services. It will eventually be implemented within the application framework so that other applications can use the ECOPS services via APIs.

4.4 Evaluation of ECOPS

In this section, we present the evaluation results of ECOPS in terms of energy efficiency and location accuracy. We have implemented an ECOPS Android application and used several Android smartphones including Samsung Galaxy Nexus S running

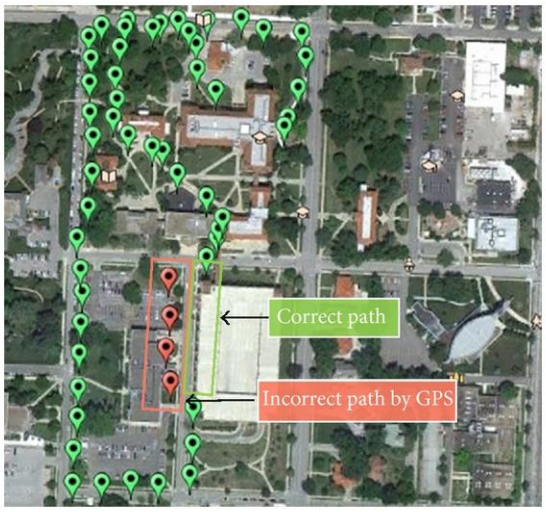


Figure 4. 8: GPS trace obtained by smartphone

Android version 2.3.6 and two LG Optimus V running Android version 2.2.2.We have turned the GPS off on some of the devices to mimic heterogeneous devices.

We start with the validation of smartphone GPS accuracy and propagation model. As a first step, we test the accuracy of commodity GPS receivers on smartphones since they are not dedicated devices like the navigation devices for positioning. We have measured the accuracy of smartphones' GPS, by walking around the Kansas City area while carrying three smartphones. As shown in Figure 4.8, the GPS collected locations are presented accurately except for a little error between tall buildings (~10m).

Next, we validate the path loss model for correlation of the distance between a WiFi signal emitter and receiver with the measured RSSI values at the signal receiver for both indoor and outdoor environments. We compared the measured RSSI value with the

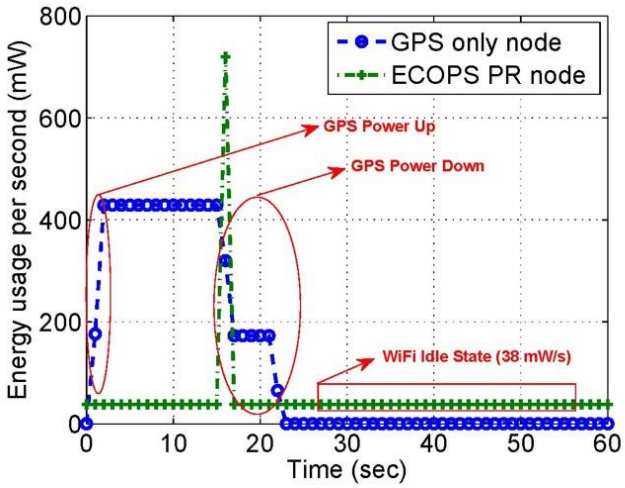


Figure 4. 9: Energy usage of GPS versus ECOPS PR

theoretical RSSI value from the path loss model. As RSSI values often vary at each time of measurement for a given location, we used an averaged RSSI value with multiple samples (e.g., 1,000 samples within a few seconds). In Figures 4.10 and 4.11 we compare the measured RSSI with the theoretical RSSI while varying the distance between PB and PR; both inside a building and in outdoor environments are shown, respectively. The theoretical RSSI values are derived from equation for path loss propagation model [88]. The dotted blue line shows the measured average RSSI values, and the solid green line represents the theoretical RSSI values at the corresponding distances. The system loss factor value (A) is set to 30. For the indoor environment, since we measured the RSSI between two devices while they were in the line-of-sight, we set the system loss factor (n) to 0.6. For the outdoor environment, we used n = 1.9. As evidenced in the figures, we observe that the path loss model works well for us in estimating the distance.

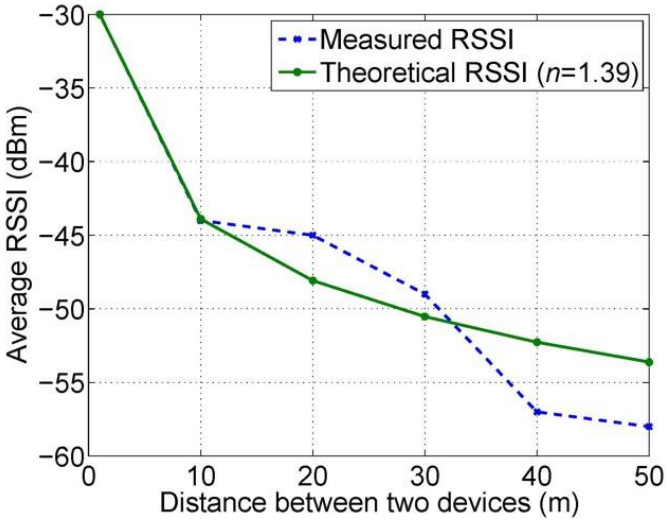


Figure 4. 10: Measured RSSI (avg. of 1,000 samples) at various indoor spots

We now compare the total energy consumption of ECOPS devices to that of devices with GPS only scheme in various settings. First, we compare the energy consumption of a node that is ECOPS PR with a node using only GPS at per second granularity as illustrated in Figure 4.9. This power consumption profiling was done using PowerTutor [89].The GPS uses 429 mW/s continuously once it is powered up and takes several seconds to power down which adds up to the energy consumption. Meanwhile, the WiFi module once powered up uses 720 mW/s in an active state and 38 mW/s when in an idle state. During the experiment, for the same operational time of one minute, an ECOPS PR node uses only 3000 mW of energy in total whereas the GPS-only node uses 7432 mW of total energy. This clearly shows that an ECOPS PR is more energy efficient than a GPS-only node. These values are for an LG Optimus V model in particular, and similar for most smartphones.

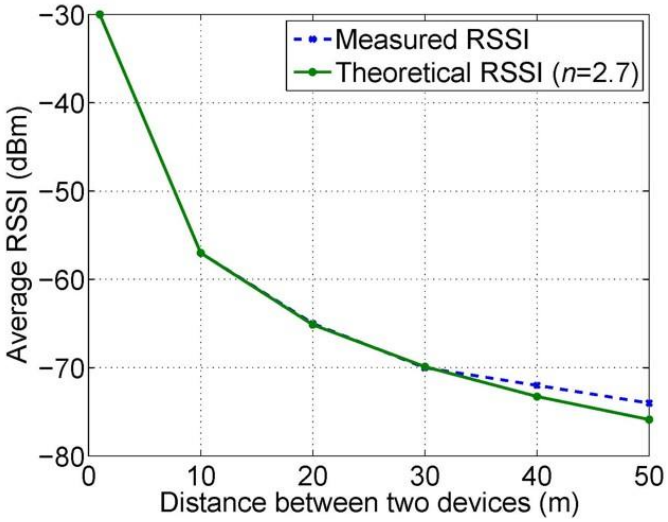


Figure 4. 11: Measured RSSI (avg. of 1,000 samples) at various outdoor spots

Next, we contrast the energy consumption of a node that is ECOPS PR with a node using only GPS while varying the operational time with 1 minute increments as illustrated in Figure 4.12.We do this experiment to analyze the effectiveness of ECOPS over a duration of time. It shows that ECOPS is increasingly energy efficient with the elapsed time over the GPS only scheme.

In Figure 4.13, we compare the energy consumption of nodes that are ECOPS PR with nodes using only GPS while varying the number of devices in the network. We do this experiment to analyze the energy efficiency of ECOPS as the number of devices in the network scales. Note that for the ECOPS PR scheme, the PRs receive GPS data from three PBs and their energy consumption is accounted for in the results. The energy efficiency

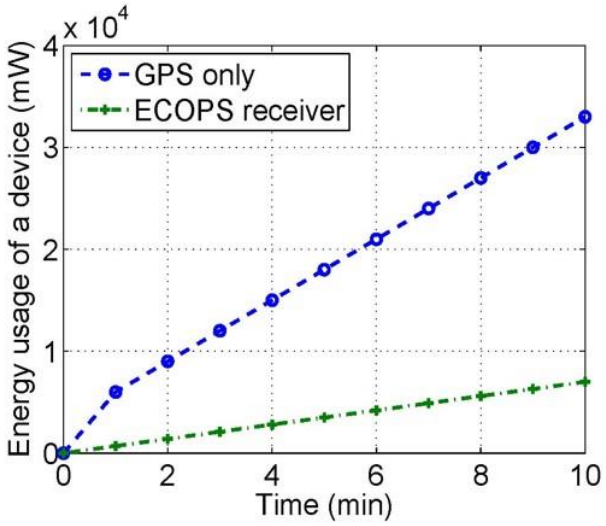


Figure 4. 12: Comparison of individual node energy consumption: GPS versus ECOPS PR

of ECOPS compared with the GPS only scheme is clear from Figure 4.13 and becomes increased substantially as the number of devices in the network scales.

Next, we evaluate the location accuracy of ECOPS as compared to that of GPS, WPS, and Cell-ID Positioning. We tested ECOPS in a soccer field using four smartphones for the accuracy measurements. The soccer field was chosen, so that we have a clear and unhindered view of the sky, and in turn the experimental results are not influenced by the GPS position errors, and the ECOPS errors are precisely measured. We turned on GPS for three devices and turned it off for a device that acted as the PR. In order to measure the location accuracy, as illustrated in Figure 4.14, we placed the PR device at the center of the area and moved the other PB devices around multiple locations within the soccer field. The PR device computed its location using the measured RSSI values, and GPS coordinates from the PBs, and the trilateration technique described in Section 4.3.

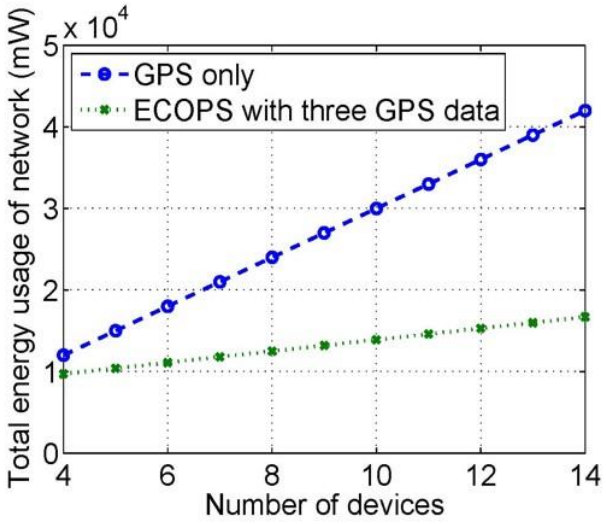


Figure 4. 13: Comparison of total energy consumption of nodes (1 min): GPS versus ECOPS

We have moved the PBs to various places around the PR and recorded the PR's computed locations. As shown in Figure 4.15, we observed that ECOPS achieves a minimum error range of 2.32 m and a maximum error range of 33.31 m. While from Figure 4.16 we can observe that nearly 60 %of these locations are within a 10 m error range and less than 10 % have an error range greater than 15 m. The results represent that ECOPS can achieve a higher location accuracy than WPS while using less energy than GPS receivers. Also, note that the error ranges we observe here are an amalgamation of the general GPS receiver error from the PBs and the distance measurement error from the RSSI values.

Finally, we compare the errors of different positioning methods in Figure 4.17. As before, a smartphone that needs positioning is located at the center of soccer field. The

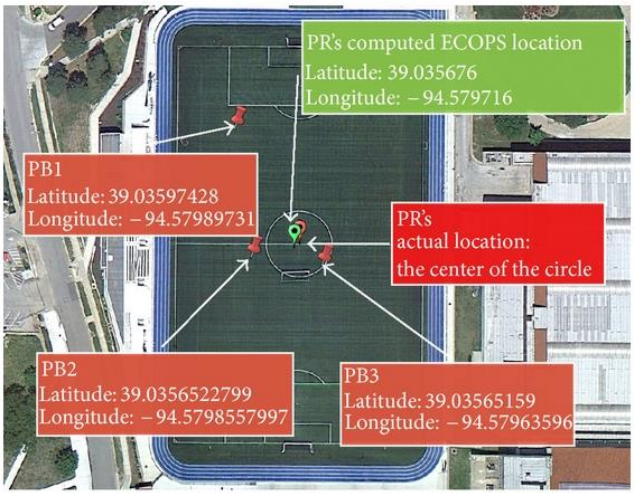


Figure 4. 14: ECOPS field experiment setup for accuracy measurements

network positioning API in Android obtains the location information either from WPS or Cell-ID Positioning. In order to ensure the Cell-ID Positioning in Android, the smartphone acquired the location from network positioning API while turning off the WiFi signal. The location information received was off by almost 300 m. Together with the location, it also suggested its own estimated error range of 1,280 m associated with it. Clearly, such information is too inaccurate to be used in most of LBS application scenarios. As for WPS, the smartphone obtained the location from Android network positioning API while turning off cellular signal. Note that WPS is not typically available in outdoor environment. Thus, we used an average WPS error from what we experimented at multiple locations in Kansas City area where WPS is available and found it to be 60m. It is the dotted blue line in Figure 4.17. While the GPS-based location information proved to be the most accurate with an error range of about 2 m, ECOPS achieved the accuracy ranging from 2.32 m to

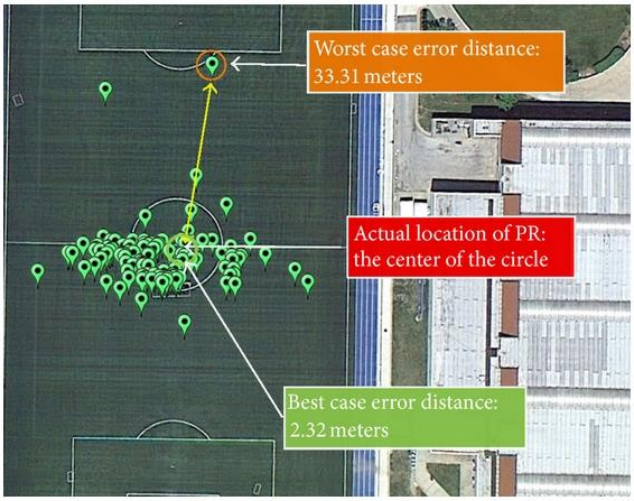


Figure 4. 15: Experiment results: points calculated with three GPS coordinates and RSSI values

33.31 m. This is better than the performance of a WPS and fairly close to GPS accuracy while saving energy costs. This encourages us to comment that even when WPS service might be available, using ECOPS will facilitate a smartphone to receive more accurate location information at the same energy cost.

4.5 Conclusions

In this chapter, we have presented an Energy Efficient Collaborative Opportunistic Positioning System (ECOPS) for heterogeneous mobile devices. Unlike existing approaches that are seeking the best available positioning method from an individual device, ECOPS facilitates collaborative environments among a set of mobile devices, and thus mobile devices benefit from their neighboring devices. ECOPS supports heterogeneous devices to maximize energy-efficiency, as a device with only WiFi can

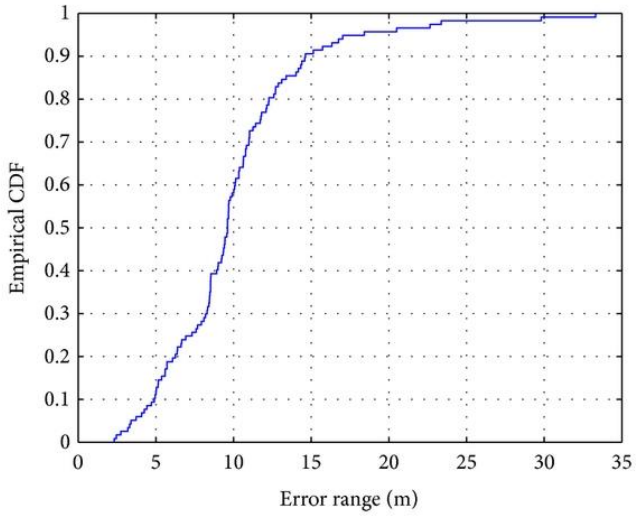


Figure 4. 16: Distribution in error range for location estimated by PR

collaborate with a few available GPS broadcasting devices via WiFi hotspot mode or WiFi Direct-based approximation. A beneficiary device may use one or more locations' information from neighbors opportunistically, depending on their availability. Furthermore, each device improves the received location accuracy via various available methods including trilateration or approximation with geomagnetic sensors. We have implemented an ECOPS prototype application on Android 2.3.6 and 2.2.2 and have tested it with various types of Android mobile devices. The results show that ECOPS provides accuracy within 10 m for nearly 60 % of the location estimates, and within 15 m for more than 90 % of them. ECOPS also offers significantly more energy efficiency than a GPS-only scheme, while overcoming various service limitations.

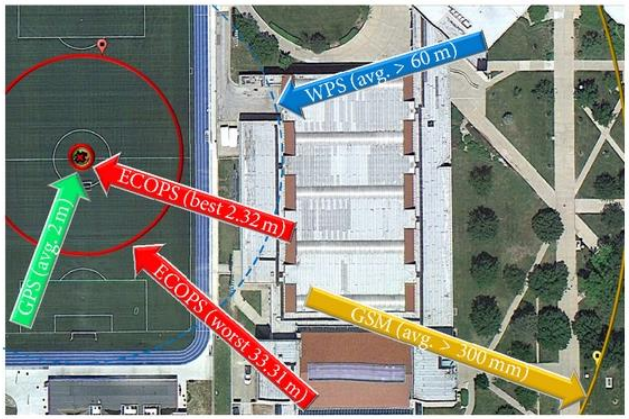


Figure 4. 17: Accuracy comparison: ECOPS, GPS, WPS, and GSM-based positioning

CHAPTER 5

REDUCING AND BALANCING ENERGY CONSUMPTION IN INDISTRIAL INTERNET OF THINGS (IIoT)

The Industrial Internet promises to dramatically improve productivity and efficiencies in the production process and throughout the supply chain. Processes in the future are likely to govern themselves, with intelligent machines and devices that can take corrective action to avoid unscheduled breakdown of machinery. Individual parts will be automatically replenished based on real time data. Every handheld digital device in the factory will report the status of every fixed device, giving personnel mobile access to real-time, actionable information [90]. Wearable pervasive devices, including sensors will track the location and work load of each employee in the factory that in turn will improve efficiencies and provide 24 by 7 visibility. These are only a few examples of the huge power of the Industrial Internet.

Within the Industrial Internet, IoT systems and their application have gained unprecedented popularity and proliferation in recent times. A recent report projects the IoT systems to increase in their economic impact from the current $3.9 trillion to $11.1 trillion a year by 2025 [1]. This significant economic impact is a direct result of connecting over 50 billion devices to the Internet. One part of this growth focuses on connecting everyday objects being used by humans to the Internet. The potential of creating such Internet connected devices or IoT devices is huge. IoT devices offer various avenues that

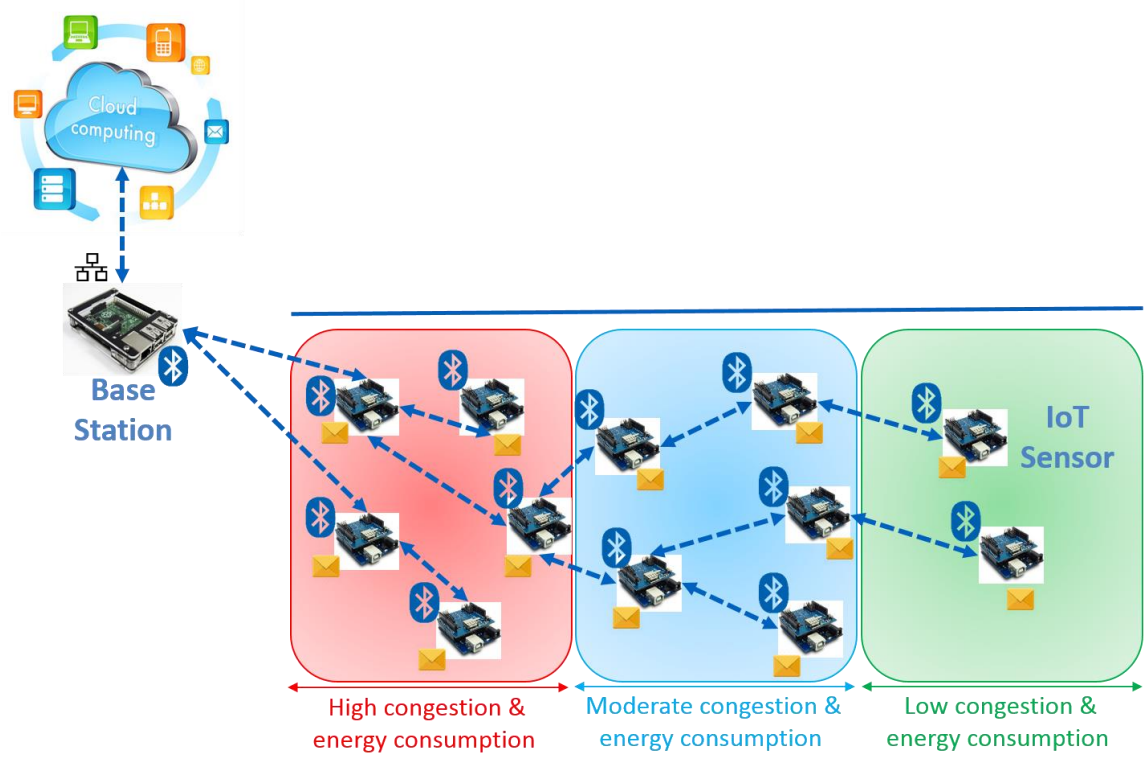


Figure 5. 1: Typical Vanilla System architecture in manufacturing environment

make human interactions with the machines possible. Some examples of such applications are in the field of healthcare by monitoring the vital signs of a person via wearable devices, home automation, home security, personalized care and products, smart vehicles, etc. While such applications offer a huge potential, the other aspect of IoT which is even more critical, involves connecting the machines in industries to the Internet, with each other and with the work force in a plant. This philosophy forms the basis for Industrial Internet of Things (IIoT) [2].

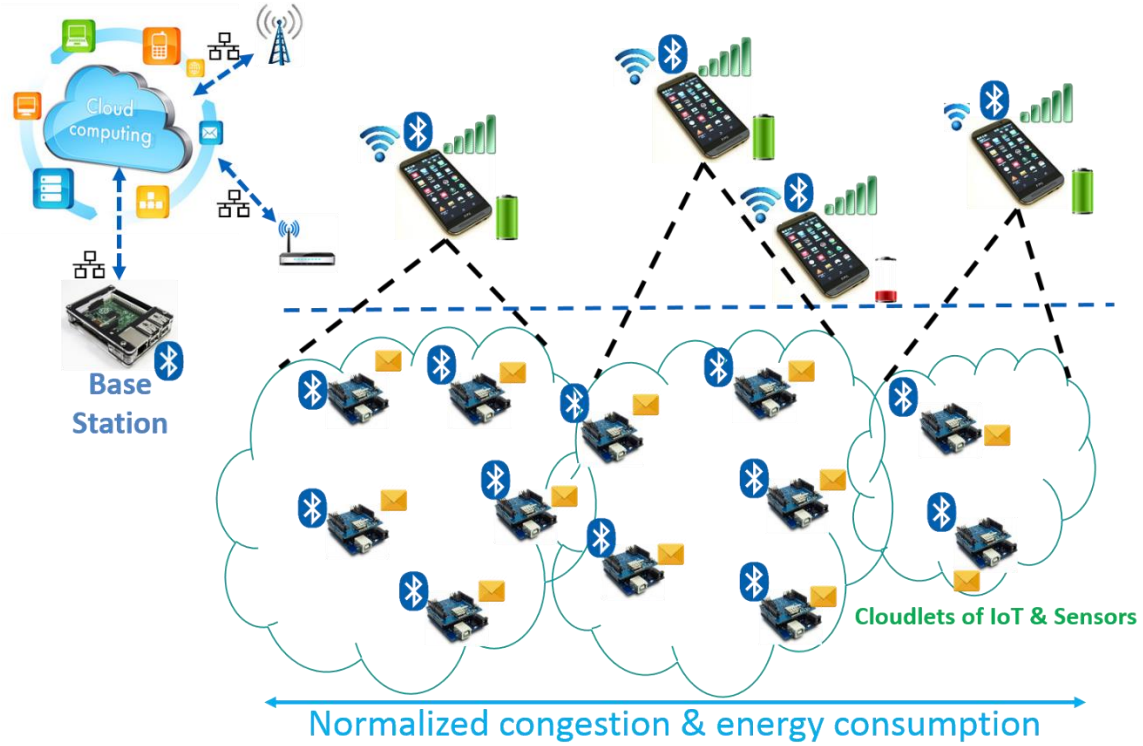


Figure 5. 2: The HOLA System architecture

The existing state-of-the art machines used for manufacturing already support analog or digital sensing that is reported to a central control room for monitoring over wired Ethernet systems [91]. However these systems are still typically not connected to the Internet. Retrofitting existing aging machines with plug-and-play IoT devices offers a cost effective solution over replacing the machines. Having such prognostics capabilities by monitoring the vibrations in mechanical bearings of the machine with vibration sensors and excessive heating with temperature sensor will reduce the downtime by optimizing maintenance [92]. Tracking of the inventory during the manufacturing process can be

Algorithm 5. 1: HOLA IoT Device Operation

IoTDeviceOperation()

1: At start time, initiate all on-board sensors;

2: Extract HOLA IoT device ID (H_{id});

3: while HOLA IoT device operational do

4: Extract RFID of product being processed (C_{rfid});

5: Extract current temperature at the machine (C_{temp});

6: Extract current humidity at the machine (C_{hum});

7: Extract current vibrations at the machine (C_{vib});

8: HIP = (H_{id}, C_{rfid}, C_{temp}, C_{hum}, C_{vib});

9: if Base Station device in range then

10: Transmit HIP to Base Station device;

11: else if HOLA smart device in range then

12: Transmit HIP to HOLA smart device;

13: else if Downlink HOLA IoT device in range then

14: Transmit HIP to HOLA IoT device;

15: end if

16: if $N_{minTemp} <= C_{temp} <= N_{maxTemp}$ & $N_{minHum} <=$ Chum $<= N_{maxHum}$ & $N_{minVib} <= C_{vib} <= N_{maxVib}$ then

17: $S_T = S_{maxT}$;

18: else

19: if $S_T > S_{minT}$ then

20: S_T --;

21: end if

22: end if

23: end while

achieved with Radio Frequency Identification (RFID) technology. IoT devices such as the above sensors serve as enablers in smart supply chain and smart manufacturing. The system architecture for such a deployment of IoT devices in a manufacturing environment is illustrated in Figure 5.1. We will refer to this system architecture as the Vanilla System.

In the Vanilla System, the main components are the IoT devices, Base Station, and the Cloud service provider. The IoT devices in such deployments are typically powered by microcontrollers such as Arduino [93]. The plug-and-play nature of the devices requires them to use batteries as a source of energy. To conserve energy, the IoT devices use a low power wireless communication protocol such as Bluetooth. The IoT devices collect data from their sensors and send it to the Base Station (BS). The Bluetooth protocol has a short communication range of approximately 10 m. A typical manufacturing factory has a rectangular shape with typical dimensions of 1000 m × 900 m [94], and the BS is typically located at one end of the plant. In order to be able to reach the BS, the IoT devices form a Peer-to-Peer (P2P) multi-hop network. Thus the IoT devices not only sense and report data collected from the sensors, but also the data arriving from neighboring nodes down the link that needs to be forwarded to the BS over the Bluetooth interface. The BS, for example, could typically be powered by a Raspberry Pi device [95]. The BS collects all the

Algorithm 5. 2: HOLA Smart Device Operation

SmartDeviceOperation()

1: while Smart device enrolled in HOLA operation do

2: Extract HIP received from HOLA IoT Device;

3: Extract smart device location;

4: if Elapsed Time (ET) > Decay Time (DT) Or Current Location (CL) not stored then

5: Extract bandwidth, delay and loss for all available communication links L_{BDL} = [bandwidth, delay, loss];

6: Determine and set for current location C_L an optimal link $L_{Optimal}$ = Compare($WiFi_{BDL}$; LTE_{BDL}; $3G_{BDL}$;$Bluetooth_{BDL}$);

7: end if

8: Transmit HIP over $L_{Optimal}$;

9: end while

sensor data from the IoT devices over Bluetooth interface and transmits it to the Cloud for further processing over wired Ethernet interface. The Cloud is powered by an analytics platform. Some examples of IoT platforms are the TCS Connected Universe Platform (TCUP) [96] and the Splunk platform [97] for machine data.

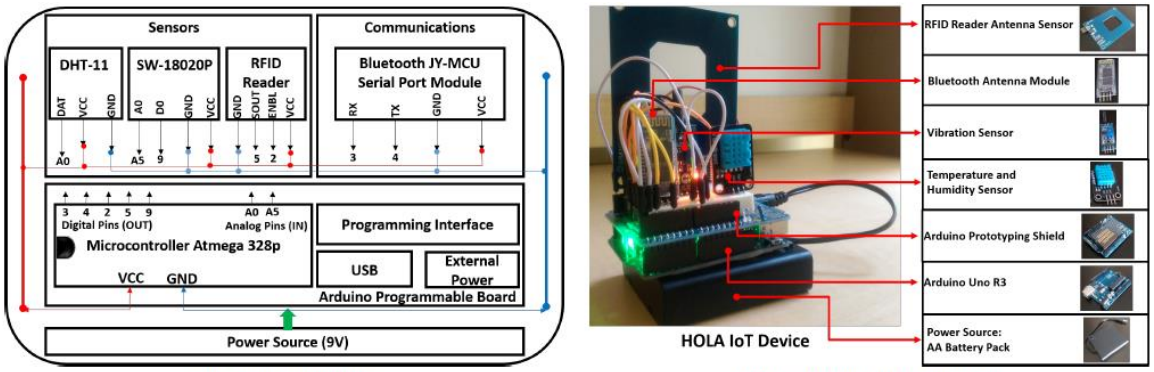
We observe that the network topology in the Vanilla System leads to low energy efficiency of the IoT devices. Specifically, we observe that the nature of the network

Table 5. 1: Comparison of various wireless radio interfaces

Wireless Protocol	Range (m)	Bandwidth	Energy Efficiency
Bluetooth	10	Low	High
WiFi	100	High	Medium
3G/4G LTE	5000	Medium to High	Low to Medium

topology leads to increased energy consumption and geo-physically skewed energy consumption of the IoT devices. The IoT devices at one end of the network sense and transmit only their sensor data. This results in low congestion and low energy consumption in these IoT devices. However the IoT devices at the center of the network are not only sensing and reporting their sensor data, but also that of the IoT devices from uplink (i.e., located at farther end of the network). This leads to moderate congestion and energy consumption. The IoT devices closer to the BS have to sense and transmit their own sensor data and also transmit the sensor data arriving from the rest of the network. This leads to high congestion and energy consumption in these IoT devices. The additional transmission responsibilities result in the IoT devices operating Bluetooth antenna for long durations. This, in turn, increases the energy consumption of the IoT devices that are close to BS.

High energy consumption in IoT devices in an Industrial Internet setting is not desirable since it results in reduced network lifetime and increased carbon footprint. Skewed or uneven energy consumption is not desirable as it makes planned maintenance of IoT devices for battery replacement challenging and increases the overall down time. With this in mind, in this paper, we propose a Heuristic and Opportunistic Link selection Algorithm (HOLA), for IoT systems that improves the energy-efficiency of IoT systems by

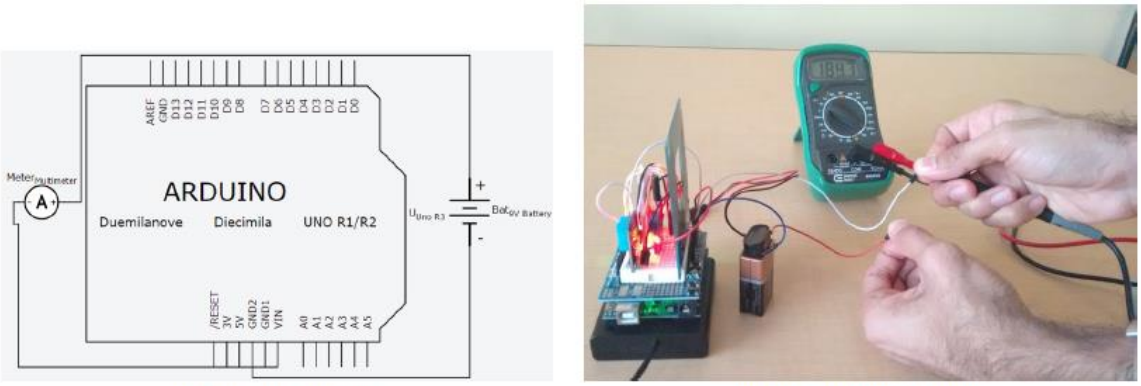


(a) Circuit diagram (b) Prototype implementation

Figure 5. 3: The HOLA IoT device

reducing the overall energy consumption and balancing it across the network. HOLA achieves this energy-efficiency by opportunistically offloading the IoT device data to smart devices (e.g., smart phones, tablets, etc.) being carried by the workforce in factory settings. Further, these smart-devices with multiple radio links such as Bluetooth, Wi-Fi, and 3G/4G LTE heuristically determine the best link to transmit the data to the Cloud based on the quality and energy cost of the link. Our experimental and simulation studies validate that HOLA can improve the energy efficiency of IIoT systems by reducing the overall energy consumption and balancing it across the network.

Our contributions in this chapter are as follows: we observe and report the high and geo-physically skewed energy consumption in IoT system networks, we then propose the HOLA system that improves the energy-efficiency of IoT systems by reducing overall energy consumption and balancing it across the network, we design and prototype the



(a) Circuit diagram (b) Experimental setup

Figure 5. 4: HOLA IoT device power consumption

HOLA IoT device, and perform experiments and simulation studies to validate energy-efficiency of HOLA.

The rest of this chapter is organized as follows. The detailed explanation of the proposed HOLA system is presented in Section 5.1. The prototyping of HOLA IoT devices and performance evaluation of the HOLA IoT system is presented in Section 5.2. In Section 5.3, we discuss about the existing state-of-the-art techniques. And with Section 5.4, we conclude this chapter.

5.1 HOLA Approach

Modern smart-devices such as smartphones and tablet computers powered by various operating systems such as Android, Windows and iOS are equipped with multiple radio interfaces to connect to the Internet and other wireless devices. Examples of such radio interfaces are Wi-Fi (IEEE 802.11 a/b/g/n/ac), Bluetooth (IEEE 802.15.x), and cellular

Table 5. 2: HOLA IoT device power consumption

Activity	Current Draw (mA)	Power Consumption (mW)
Arduino Idle Operation	47.1	423.9
1 Sensor Active - Vibration Sensor	55.5	499.5
2 Sensors Active – Vibration, Temp & Humidity Sensor	58.2	523.8
3 Sensors Active – Vibration, Temp & Humidity Sensor, RFID Sensor	184.1	1656.9
Bluetooth Transmit & Receive	203.5	1831.5

3G/4G LTE. These wireless interfaces have unique characteristics in terms of operational range, energy consumption, bandwidth, and availability. These key characteristics are illustrated in Table 5.1 [5]. In the proposed HOLA system, we exploit these multiple wireless radios equipped with the smartphones carried by the workforce in the factory settings to offload the IoT device data.

The system architecture for HOLA is illustrated in Figure 5.2. In the HOLA system, the IoT devices carry out the sensing in an intelligent fashion. These devices engage in efficient filtering and fusion of sensor data to reduce the amount of data that needs to be transmitted. For example, during a regular operation, the HOLA IoT devices sense and report data collected over a one minute interval. However, when the predefined thresholds for the sensor data are breached (indicating, for example, a machine failure or other critical event), the HOLA IoT device dynamically increases the sampling and reporting rate. When it is time to report the collected sensor data, the HOLA IoT devices opportunistically offload the sensor data to an available smart phone over a Bluetooth

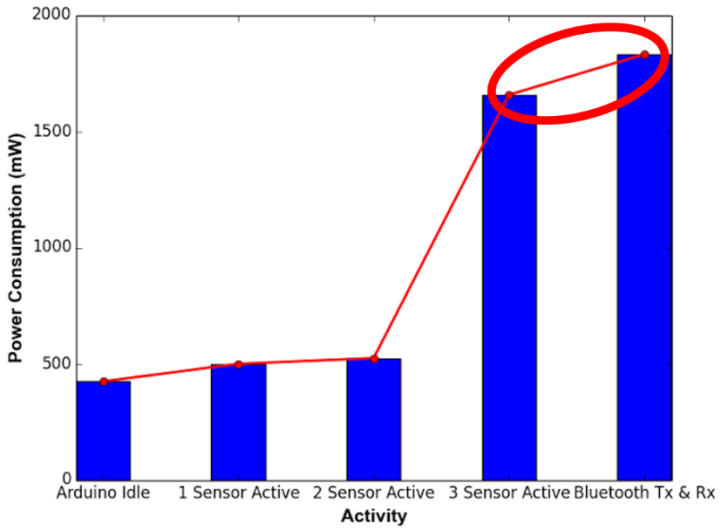


Figure 5. 5: HOLA IoT Device Power Consumption

interface. If a smartphone is not available, the HOLA IoT device offloads the data to a neighbor in the path to BS within the Peer-to-Peer network.

The detailed operation of HOLA IoT device is presented in Algorithm 5.1. The HOLA IoT device initiates all its sensors at start time, and extracts the identification number (H_{id}). This unique ID is used in the Cloud to identify the machines having problem, and the components that have been processed by the machine (identified by the RFID associated with the product being processed (C_{rfid})). During its operational lifetime, the HOLA IoT device extracts the RFID of product being processed (C_{rfid}), current temperature at the machine (C_{temp}), current humidity at the machine (C_{hum}), and current vibrations at the machine (C_{vib}). With this information, it constructs the HOLA IoT Device Information Packet (HIP) which needs to be transmitted to the Cloud. If a Base Station device is within

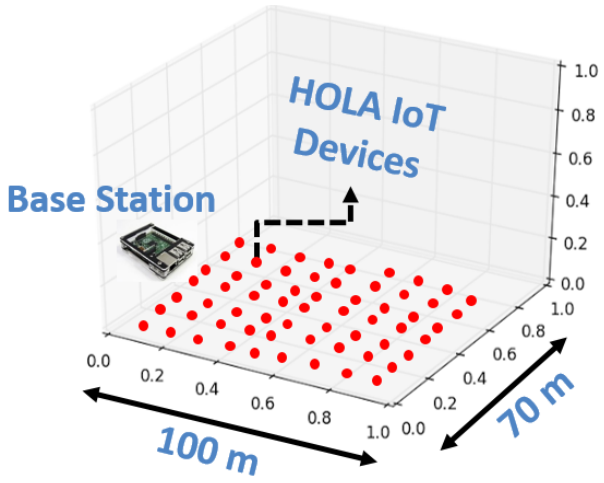


Figure 5. 6: HOLA Simulation Setup

range, the HIP is transmitted directly to Base Station device, else if a smart device participating in HOLA service is available, the HIP is opportunistically transmitted to this smart-device. If none of these are available, the HIP is transmitted to a downlink HOLA IoT device in range. Through the operational lifetime, if the sensor values fall beyond the normal operational minimal or maximum values, the sensing rate increases by reducing the sleep time (S_T) step-wise till it falls to minimum possible sleep time (S_{minT}). Otherwise, the S_T remains at maximum possible sleep time (S_{maxT}) to conserve energy.

A smart phone can potentially connect to multiple HOLA IoT devices simultaneously. This effectively creates cloudlets of IoT devices within a large deployment. It should be noted that these smartphones are typically recharged from time to time which is not possible with the IoT devices due to their nature of deployment. The primary goal of the

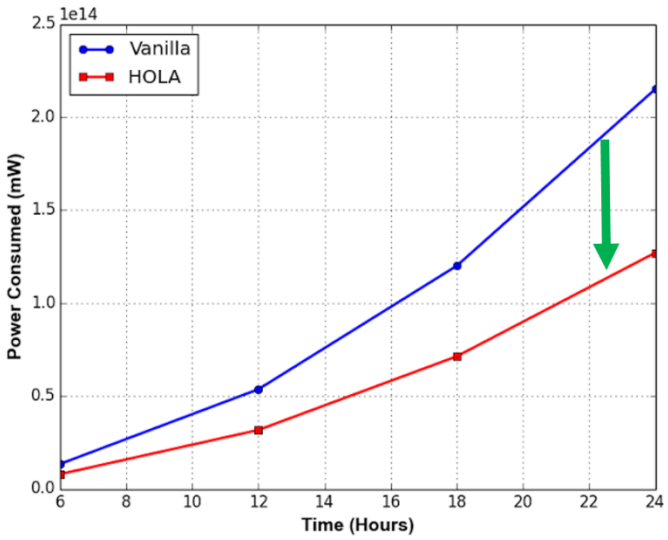


Figure 5. 7: Reduced total power consumption with HOLA

smartphones in a factory environment is to extract analytics and warnings and present it to the workforce. Based upon the data, the factory work force can take necessary actions such as, for example troubleshooting a malfunctioning machine. As result of reduced inter IoT device communication, HOLA achieves energy-efficiency by reducing the overall energy consumption as well as by balancing it geo-spatially. Geo-spatial balancing of energy consumption results in a uniform energy consumption for the IoT devices across the factory floor.

Once the data from an IoT device is offloaded to a smart phone, HOLA employs an intelligent link selection algorithm. Modern smartphones are heterogeneous in terms of availability of radio links and residual battery power. If a smartphone has low residual energy, it will not be included in the HOLA network until it is recharged. HOLA employs a

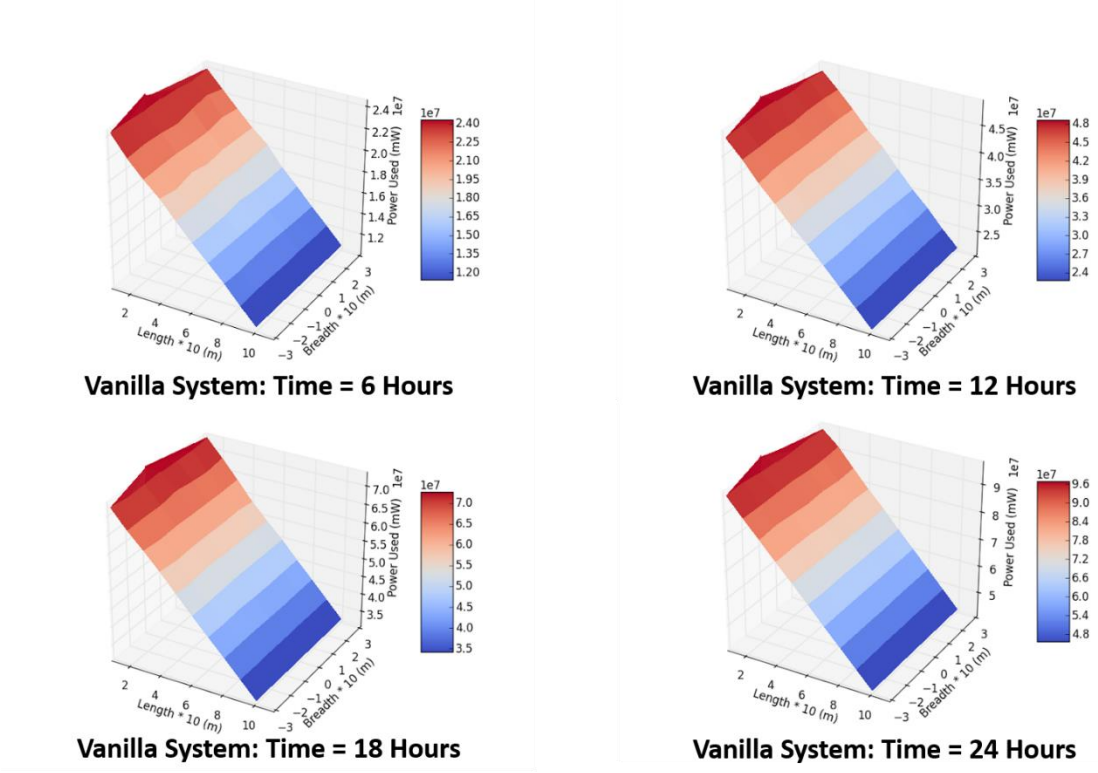


Figure 5. 8: Unbalanced power consumption at individual IoT devices with Vanilla System

set of heuristics to determine the best link (e.g., Bluetooth, Wi-Fi or 3G/4G LTE) to transmit the data over to the cloud while considering quality of the link to maintain the Service Level Agreements (SLAs), and the energy cost of using that link.

It should be noted that the Wi-Fi and the cellular radios on the smart phones consume similar amount of power per unit of operation [98], [99]. However the amount of energy used by the Wi-Fi or cellular connection for a given amount of data is a function of the available bandwidth on that link. Theoretically, Wi-Fi access points (APs) provide larger bandwidth over cellular connection. Thus, Wi-Fi can transmit same amount of data at a

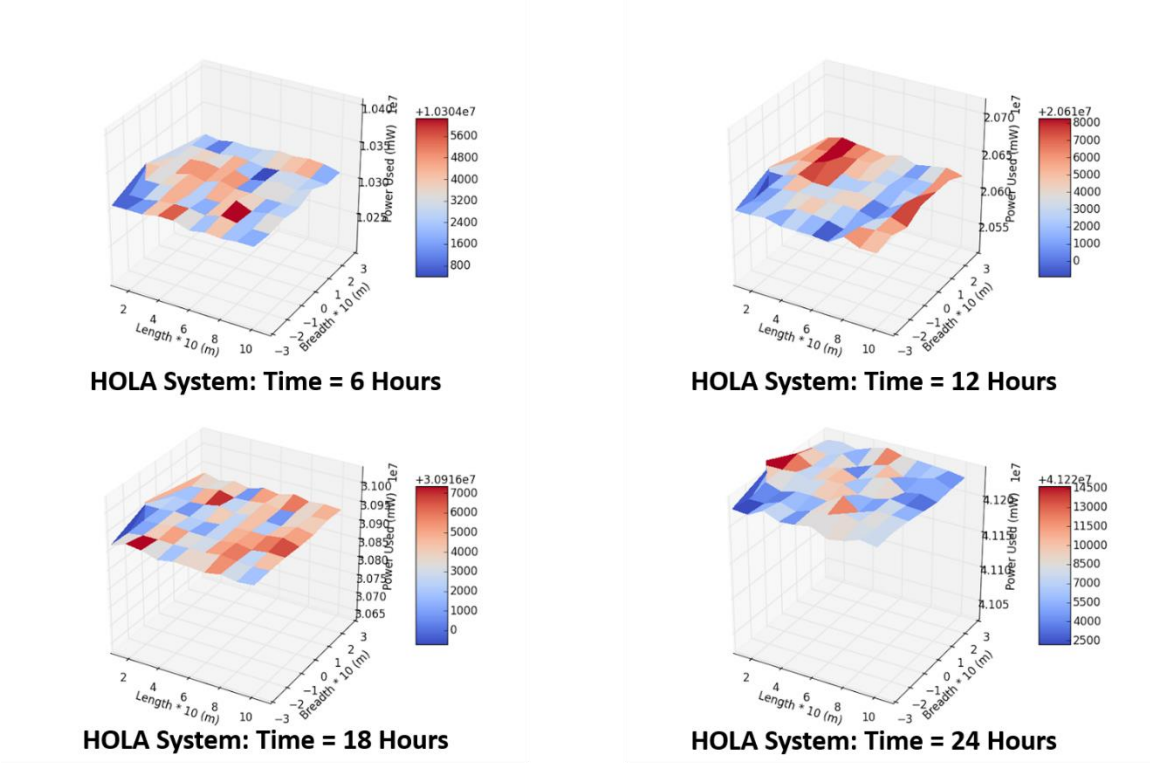


Figure 5. 9: Balanced power consumption at individual IoT devices with HOLA IoT System

faster rate as compared to a cellular connection. As a result the Wi-Fi radio is used for a shorter duration resulting in less energy usage compared to the cellular connection. However in a factory setting, there are several factors that affect the bandwidth of the Wi-Fi links. Presence of metallic structures, high temperature, or congested network due to larger number of smart phones connected to a Wi-Fi AP is likely to reduce the quality and bandwidth of the Wi-Fi link. This leads to dropped packets that results in retransmission of data.

If the number of packet retransmissions is too large, it is less costly to use the cellular 3G/4G LTE link to transmit the data to the cloud service. Hence before transmitting the data, the smartphone must be aware of the most efficient link to use. Probing the links frequently to check for available bandwidth is costly in terms of energy, and no active transmission can be carried for the duration of probing. Typically the working stations in a factory are fixed. Thus while probing the links, the smart phones in HOLA system geo-tag a particular location and associate the link to be used in its neighborhood and store this information in their database. This information can be recalled for later use, and the smartphone probes for bandwidth only if the information is not available or if it is stale. The detailed operation of HOLA smart-device is described in Algorithm 5.2.

5.2 HOLA Evaluation

We have built and prototyped the HOLA IoT device from scratch with of-the-shelf components. The prototype implementation is shown in Figure 5.3, where Figure 5.3a shows the circuit diagram of the IoT device, and Figure 5.3b shows the HOLA IoT device. The HOLA IoT device is powered by the ultralow-power Atmel ATmega 328 microcontroller. This microcontroller is programmed by the Arduino Uno R3 microcontroller board. The HOLA IoT device communicates with other IoT devices and smart-devices using the JY-MCU Bluetooth Antenna Module. We have integrated the following three sensors in the HOLA IoT device: vibration sensor, temperature and humidity sensor, and an RFID antenna sensor. The HOLA IoT device supports two important functionalities.

First, HOLA IoT devices support inventory tracking and track objects in a manufacturing or an assembly setting with RFID technology. The RFID Reader Antenna sensor reads the codes associated with RFID tags attached to the items as they go through the assembly chain. Second, HOLA IoT device can predict, detect, and report machine degradation. HOLA IoT devices use the vibration sensor to detect anomalous behavior of a machine and the temperature and humidity sensor to detect over heating of the machine.

We have studied the power consumption of the HOLA IoT device that we have built with detailed experiments. The experimental setup and circuit diagram for the power consumption experiments are illustrated in Figure 5.4, where Figure 5.4a shows the circuit diagram of the experimental setup to measure power consumption, and Figure 4b shows the experimental setup. The current drawn by the HOLA IoT device is measured with a digital multi-meter (DMM) for 9V battery. We measure the power consumption of the HOLA IoT device for various operation scenarios as illustrated in Table 5.2. Each of these experiments have been conducted 50 times, and the average values have been reported. As can be seen from Figure 5.5, the radio frequency transmitters and receivers consume significant amount of energy in the HOLA IoT devices. The high power consumed by the Bluetooth module becomes significant when the IoT devices transmit not only their own data but also the data of their neighbors. We have tested the operation of HOLA IoT devices with Nexus 7 tablet powered by Android 5.1.2, HTC One M8 smartphone powered by Android 4.4.2, and a HP Stream 7 tablet powered by Windows 8.1. The HOLA IoT devices are not only plug-and-play, but also support cross-platform compatibility along

with third-party applications. The HOLA device successfully communicates with these smart devices to offload the sensor data from its onboard sensors. A video demo of the HOLA IoT device is available on YouTube at [100].

With the help of simulation studies we investigate scalability to study the performance of HOLA as compared to the Vanilla System. The parameters used in the simulation studies have been experimentally obtained by us. To provide realistic loss in wireless environment, we have implemented the Rayleigh Fading signal propagation model [63] with environmental noise of 95 db. The simulation setup has been created in Python with NetworkX, SciPy, and NumPy libraries. The simulation environment reflects a 100m*70m factory floor with HOLA IoT devices placed at uniform 10m interval for a total of 700 devices as shown in Figure 5.6. A duty-cycle sensing and reporting is done every 60 seconds. The BS is located at one end of the setup. We perform sensing activities for a 24 hour duration with the Vanilla System and the HOLA IoT system. For simulation of the HOLA IoT system, we assume that each of the HOLA IoT devices have access to a smartphone to offload their sensor data. The smart phones use 800 mW of energy at the radio link to forward data from each of the sensors to the Cloud. The power consumption values have been experimentally obtained with PowerTutor [101]. Our future work aims to observe the effects of varying smartphone density, and its impact on overall energy efficiency.

In Figure 5.7, we plot the Time on x-axis vs Power Consumed on y-axis, and observe the total energy being consumed by the IoT devices for the Vanilla System and HOLA IoT System during the 24 hour operational duration. From Figure 5.7, we can see that HOLA

successfully reduces the total energy being consumed by the IoT devices in the network as compared to the Vanilla System. HOLA is able to reduce the total energy consumption of IoT devices by reducing the inter-IoT device communication and opportunistically offloading the sensor data to smart devices. Further we see that, as time progresses, the energy efficiency of HOLA is more effective as compared to the Vanilla System.

We observe the energy being consumed individually at each of the IoT device in the network during the 24 hour operational duration. In Figure 5.8, we observe that in the Vanilla System the IoT devices have a highly skewed energy consumption. As time progress, uneven power consumption becomes more severe. With the HOLA IoT system, the IoT devices have a balanced power consumption across the network as illustrated in Figure 5.9. HOLA geo-spatially balances the power consumption of the IoT devices since the IoT devices closer to the BS do not have to transmit the data from the IoT devices that are farther away from the BS. Thus, with simulation with realistic power consumption values, we demonstrate that the HOLA IoT system not only successfully reduces the total energy consumption, but also balances it across the IoT device network.

5.3 Related Work

Energy-efficiency is one of the important performance parameters of an IoT system. Industrial IoT (IIoT) applications have even further stringent requirements for network lifetime and delays [102]. In literature, researchers have proposed numerous techniques to improve energy-efficiency of IoT systems. These techniques can be classified as either duty cycling of sensor nodes, efficient filtering, and fusion of sensor data to reduce

network traffic, and using a mobile ferry to collect IoT sensor data, which again reduces the network traffic.

With duty cycling, the energy conservation and increased network lifetime are achieved by alternating the operational mode of the IoT devices between active and dormant state [102], [103], [104], [105]. They use the ability of an IoT device to operate in various modes to reduce the power being consumed. Examples of such duty cycling can involve powering down the IoT device, putting it in sleep mode where the radio is still active, or putting the IoT device in a deep sleep mode where the radio is turned off and is activated at predefined intervals to listen from the neighbor IoT devices. The drawback of duty cycling is that it could reduce the area being monitored if the deployment is not dense and also requires highly synchronized clocking to wake up the IoT device.

Efficient filtering and sensor data fusion techniques [106], [107] reduce the amount of data that is being transmitted across the network. Since the amount of data being transmitted by the radio of the IoT device is reduced, the radio itself has to be powered for a shorter duration of time than what it would have been normally. This leads to reduced power consumption at the IoT devices. While such sensor data filtering and fusion techniques are extremely efficient and successful at reducing the power being consumed at the IoT devices, they also have drawbacks. Such techniques are not effective when regulatory requirements impose finer granularity of data being reported to satisfy the SLAs.

Mobile ferry based techniques [108], [109] use a specialized IoT device that can move across the IoT network. This mobile ferry travels around the network visiting the IoT devices to receive the sensor data collected by them. Once it has collected the data from the entire network, it returns to the BS to offload the data before embarking on the travel again. Such techniques require the IoT devices to have a large buffer to store the data till the arrival of the mobile ferry which is costly. While using a mobile ferry works well for delay tolerant networks, it is not well suited for IIoT applications where, for example, a machine failure or degradation needs to be reported in real-time.

The proposed approach HOLA on the other hand, effectively exploits the smartphones and other smart devices used by the workforce in industry settings to opportunistically and heuristically offload the sensor data collected by the HOLA IoT devices. Our experimental and simulation studies confirm that HOLA achieves significant energy-efficiency by reducing the overall energy consumption of the IoT devices, and distributing it evenly across them.

5.4 Conclusions

In this chapter, we have proposed HOLA that improves the energy efficiency of IIoT systems by reducing overall energy consumption and balancing it across the network. HOLA achieves energy-efficiency by opportunistically offloading the IoT device data to smart devices being carried by the workforce in factory settings. We validate the efficacy of HOLA with extensive practical experiments backed with simulation studies.

We have designed and prototyped the HOLA IoT devices with Arduino. The HOLA IoT devices serve as an enabler to IIoT applications for smart manufacturing and smart supply chain. With the help of practical experiments, we have measured the energy consumption of the HOLA IoT devices across various operational scenarios and communication settings.

CHAPTER 6

OPTICAL WIRELESS UNLOCKING FOR SMART DOOR LOCKS USING SMARTPHONES

With the recent rapid advancements in Internet of Things (IoT) technologies, one of the applications being researched is smart door lock (SDL) systems. Smart door locks are intended to offer ease of access, easy key or access sharing as well as high security. These smart lock systems can be categorized into three broad types - biometrics, smart tags, and smartphones. However they pose issues of usability, reliability as well as security.

Biometrics-based smart door locks [110, 111] rely on the unique physical characteristics of humans such as fingerprints, facial recognition and retina to grant access to authorized users. Such biometric-based techniques are not only computationally intensive but also hard to replace once compromised. In spite of advances like liveliness detection algorithms, biometric based techniques are prone to easy security breaches [112]. While smart tags [113] utilize Radio-frequency Identification (RFID) or Near Field Communication (NFC) technology, smartphones [114, 115] use Wi-Fi, Bluetooth, or NFC to provide keys to the smart lock in order to unlock it. They can thus be classified to use radio frequency (RF) technologies. Such RF technologies are susceptible to snooping attacks [116] and also cause RF smog.

In this chapter, we propose an optical wireless unlocking for SDL. We have designed and prototyped a SDL system named OptLock. OptLock accepts an optical wireless signal (OWS) which contains the encoded one-time-password (OTP) key via its onboard infrared (IR) sensor to unlock. This challenge-response based OWS is transmitted by the user

Table 6.1: Characteristics of communication mechanism

Communication Mechanism	Range (m)	Energy Efficiency	Radiation Pattern	RF Smog
Wi-Fi	~100	Very Low	Omnidirectional	Yes
Bluetooth	~10	Low	Omnidirectional	Yes
NFC/RFID	~0.1	Very Low	Omnidirectional	Yes
OWC (VLC)	~0.1	High	Highly Directional	No
OWC (IR)	~10	High	Directional	No

through a smartphone via its onboard IR light emitting diode (LED). In the absence of an onboard IR LED, an external dongle containing an IR LED can be easily connected to the smartphone. This hardware we designed is powered through the smartphone's 3.5 mm headphone jack. Optical wireless communication (OWC) with IR enables energy-efficient, and comfortable range line-of-sight communication (which is highly desirable is such security applications). Also, it does not contribute to the negative effects that are caused by the RF smog. The data rate offered by IR (~4000 bps) is more than sufficient for an application like OptLock that needs to send a 128 bits long key in under a second.

Our experiments and analysis validate that OptLock offers a fast and efficient unlocking experience which is highly secure, and successfully thwarts various attack scenarios [7]. OptLock offers the physical security of traditional door locks without the need to carry extra keys. The inbuilt challenge-response and one-time-password scheme enables better security over existing smart locks along with easy key sharing among users.

The rest of this chapter is organized as follows. A detailed explanation of the proposed OptLock system is presented in Section 6.1. The prototype implementation along with performance evaluations are explained in Section 6.2. Finally, we conclude the chapter in Section 6.3.

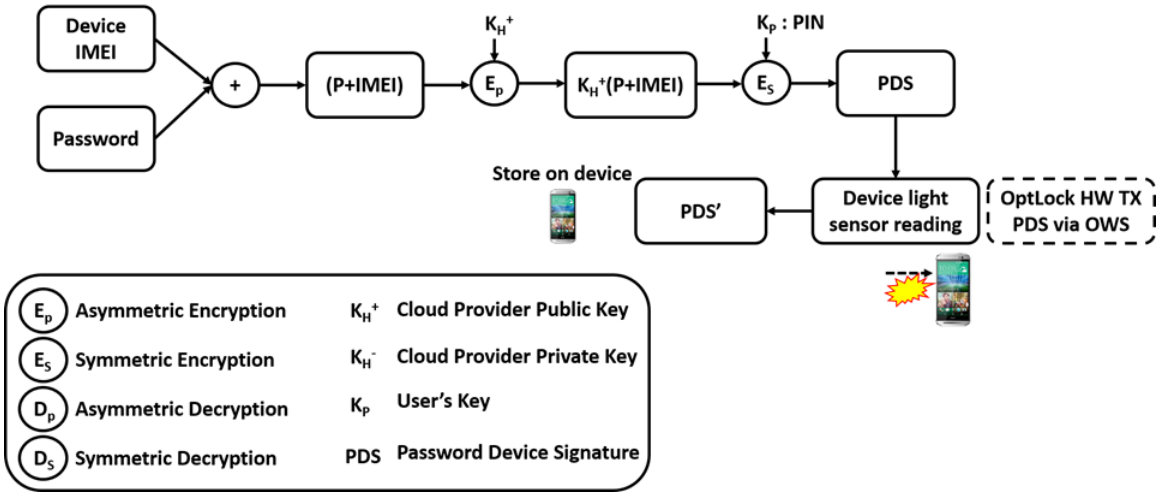


Figure 6.1: OptLock: Key distribution phase

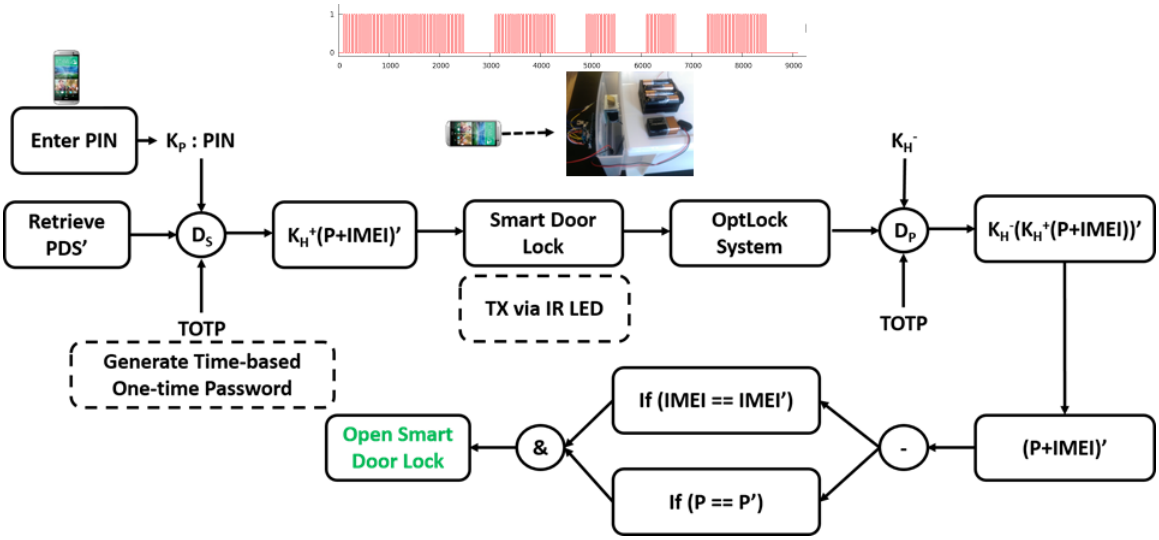


Figure 6.2: OptLock: Authentication phase

6.1 OptLock Approach

An OptLock SDL operation takes the following process. During the key distribution process, the user sets up the SDL to be operated with an authorized smartphone. First, as illustrated in Figure 6.1, the authorized smartphone's unique identifier (such as the IMEI

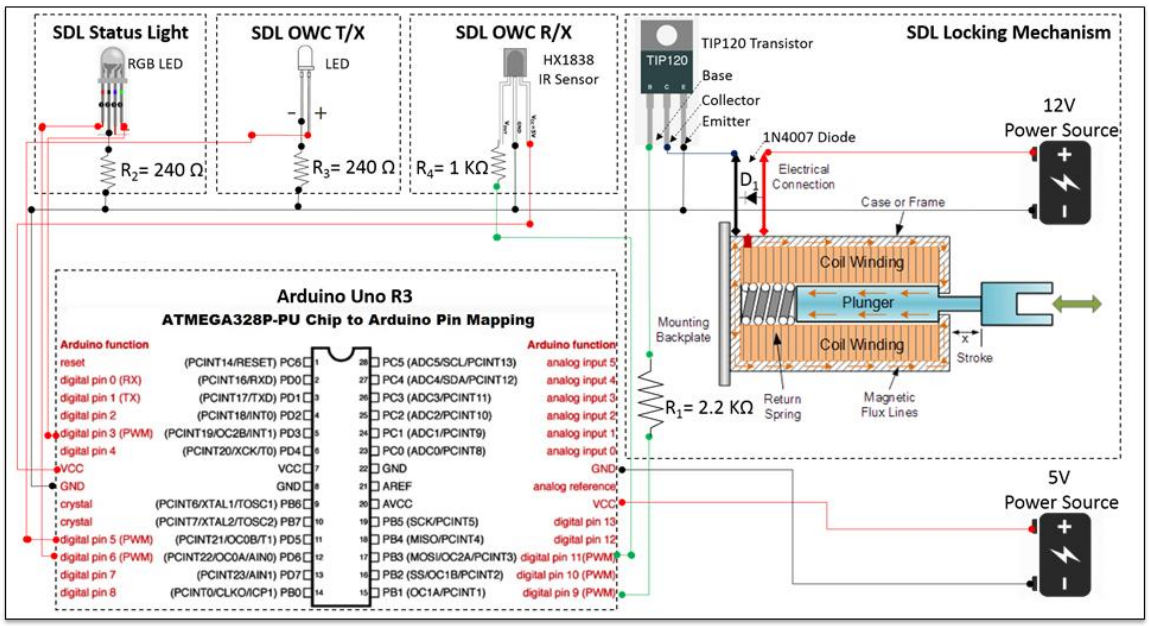


Figure 6.3: OptLock: Prototype circuit diagram

or MAC) are concatenated with the user's password. This concatenation is encrypted with the cloud provider's public key (K_H^+) for the user. This is further encrypted with symmetric encryption function E' that takes the user's personal identification number (PIN) as it's key to produce the Password Device Signature PDS. This PDS is transferred to the smartphone by the OptLock hardware using OWS, and stored locally as PDS'.

During the authentication phase the user must first prove that he/she is the actual owner of that smartphone that is authorized to unlock the SDL. This is achieved using the

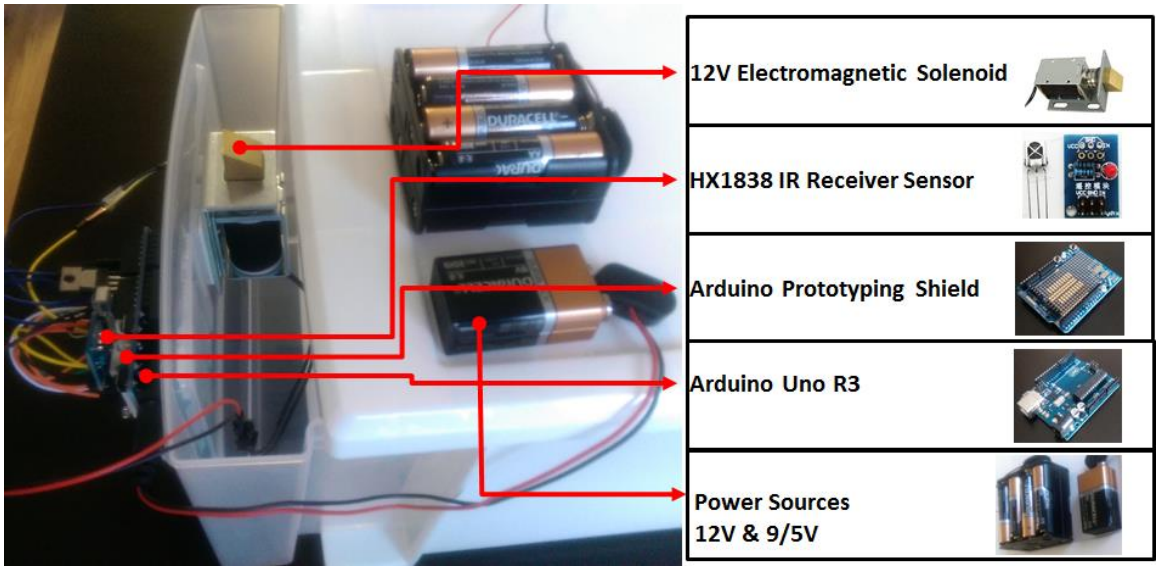


Figure 6.4: OptLock: Prototype implementation

PIN of the user as illustrated in Figure 2.6. At the time of unlocking the OptLock SDL, the user's smartphone retrieved the PDS' that is stored locally and uses the PIN entered by the user (KP) along time-based one-time password (TOTP) function to symmetrically decrypt the PDS'. The resulting K_H^+(P+IMEI)' is transmitted to the OptLock SDL by the smartphone using its IR LED. The OptLock SDL then asymmetrically decrypts it using its private key for the user while applying the TOTP function to recover the (P+IMEI)'. A disjoin function further recovers the P' and IMEI'. If the P' matches with the original password (P) on file for the user with the IMEI matching the IMEI' of the smartphone being used, the OptLock SDL successfully unlocks.

Thus, OptLock offers the physical security of traditional door locks without the need to carry extra keys. The inbuilt challenge-response and one-time-password scheme

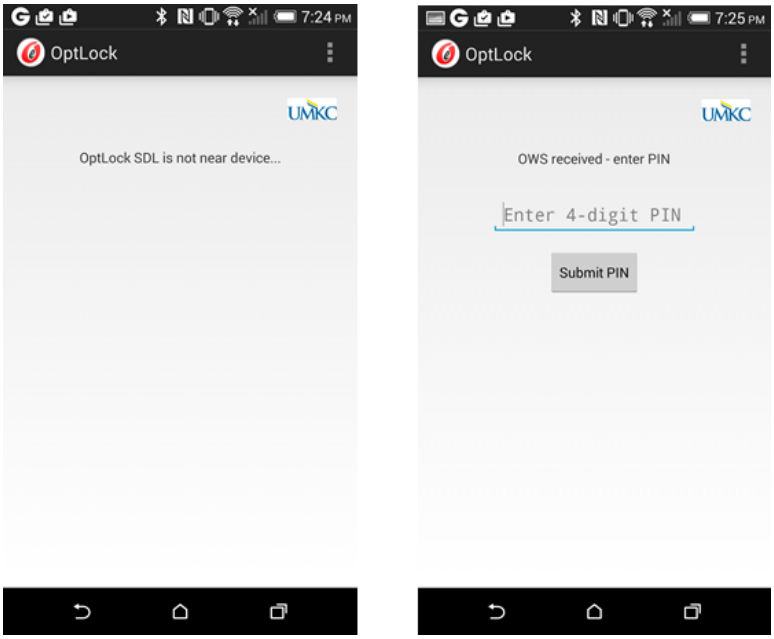


Figure 6.5: OptLock: Application screenshots

enables better security over existing smart locks along with easy key sharing among users. OptLock also protects against the threat from a stolen smartphone with challenge-response enabled by requiring the entry of a PIN to operate the SDL. An incorrect PIN results in the failure to match the password and IMEI of file.

6.2 OptLock Prototype Implementation and Evaluation

In this section we explain the implementation and experimental settings used to validate the energy-efficiency of OptLock SDL system. We built and programmed a prototype SDL hardware using the ultra-low power microcontroller ATmega328P by Atmel [18]. The ATmega328P microcontroller was programmed using the Arduino Uno Revision 3 [19] microcontroller board. The OptLock SDL receives IR OWS from the

Table 6.2: OptLock Evaluation - Power consumption

Activity	Current Draw (mA)	Power Consumption (mW)
Arduino Idle Operation	47.1	423.9
Arduino With IR Receiver (HX1838)	48.11	433.9
Arduino With Bluetooth (JY-MCU)	66.5	598.5
Arduino With Wi-Fi (CC3000)	135	1215

smartphone via the HX1838 IR sensor. A 12V electromagnetic solenoid enables the locking functionality of the OptLock SDL. The OptLock SLD also has an onboard LED for transmitting data to the smartphone via its ambient light sensor, and a RGB LED that acts as a status indicator. The hardware unit is powered by a 12V battery pack for the solenoid, and a 9V battery for rest of the onboard electronics. The schematic of the circuit we built for the OptLock SDL hardware along with the block diagram of the Arduino Uno microcontroller board is shown in Figure 6.3 and the hardware SDL we built is shown in Figure 6.4.

We built the OptLock application for Android using the Android SDK. The application has been designed to transmit the OWS via its onboard IR LED once the user enters the PIN. The application also displays various status messages. The screenshots for the application are shown in Figure 6.5. We used an HTC One M8 powered with Android 4.4 to implement OptLock Android application. In the absence of an onboard IR LED, an external dongle containing an IR LED can be easily connected to the smartphone. This hardware we designed is powered through the smartphone's 3.5 mm headphone jack.

We have studied the power consumption of the OptLock SDL hardware that we have built with detailed experiments. The current drawn by the OptLock SDL hardware for communication is measured with a digital multi-meter (DMM) for 9V battery. We measure the power consumption of the OptLock SDL hardware for various communication scenarios as illustrated in Table 6.2. Each of these experiments have been conducted 50 times, and the average values have been reported. Using any form of RF communication mechanism results in usage of higher amounts of energy as compared to using an IR receiver. Thus, using IR OWC will enable the OptLock SDL hardware to operate for longer duration without having to replace the batteries.

6.3 Conclusion

We have presented a smart door lock system named OptLock. OptLock accepts an optical wireless signal (OWS) which contains the encoded one-time-password (OTP) key via its onboard infrared (IR) sensor to unlock. This challenge-response based OWS is transmitted by the user through a smartphone via its onboard IR light emitting diode (LED). In the absence of an onboard IR LED, an external dongle containing an IR LED can be easily connected to the smartphone. Our experiments and analysis validate that OptLock offers a fast and efficient unlocking experience which is highly secure, and successfully thwarts various attack scenarios.

CHAPTER 7

SUMMARY AND FUTURE DIRECTIONS

7.1 Summary

In this dissertation, we analyze in detail the various characteristics of different wireless communication methods in terms of range, energy-efficiency, and radiation pattern. We find that a well-established communication method might not be the most efficient, and other alternate communication methods with the desired properties for a particular application could exist. We exploit alternative, state-of-the-art, and complimentary wireless communication methods, including radio frequency, infrared (IR), and visible lights, through the various IoT applications we have designed and built with those.

Using Optical Wireless Communication (OWC) as a direct communication method, we have developed two IoT applications. First, we have designed and prototyped the Fast, Inexpensive, Reliable and Easy-to-use (FIRE) hardware token with the Inverse Dual Signature (IDS) which offers an Optical Wireless Authentication (OptAuth) for users authenticating on a smartphone. OptAuth offers convenient and cheap authentication process while offering strong security and defeats various attack scenarios. Second, to offer strong physical security, we have developed a smart door lock system named OptLock. OptLock accepts an optical wireless signal (OWS) which contains the encoded one-time-password (OTP) key via its onboard infrared (IR) sensor to unlock. This challenge-response based OWS is transmitted by the user through a smartphone via its

onboard IR light emitting diode (LED). In the absence of an onboard IR LED, an external dongle containing an IR LED can be easily connected to the smartphone. Our experiments and analysis validate that OptLock offers a fast and efficient unlocking experience which is highly secure, and successfully thwarts various attack scenarios.

As for WiFi RF, we exploit the WiFi Direct or Hotspot mode of Android devices to achieve direct communication for the two apps we have developed to avoid vehicular accidents with smart devices, and to estimate their location. We propose a smartphone-based Car2X-communication system, named WiFi-Honk, which can alert the potential collisions to both pedestrians and vehicles in order to especially protect the distracted pedestrians. WiFi-Honk removes the WiFi association overhead using the beacon stuffed WiFi communication with the geographic location, speed, and direction information of the smartphone replacing its SSID while operating in WiFi Direct/Hotspot mode, and also provides an efficient collision estimation algorithm to issue appropriate warnings. Our experimental and simulation studies validate that WiFi-Honk can successfully alert pedestrians within a sufficient reaction time frame, even in high mobility environments. Complementing WiFi-Honk we have developed a collaborative positioning system for smart devices which provides them with accurate location information at a fraction of the energy cost as compared to the traditional positioning approaches such as Global Positioning System (GPS) WiFi-based positioning system (WPS), or Cell-ID positioning. The Energy-Efficient Collaborative and Opportunistic Positioning System (ECOPS) facilitates a collaborative environment where many mobile devices can opportunistically receive position information over energy-efficient and prevalent WiFi, broadcasted from a few

other devices in the communication range. Our field experiments show that ECOPS significantly reduces the total energy consumption of devices while achieving an acceptable level of location accuracy.

Finally, we have used multiple modes of direct communication methods for a large scale Industrial Internet of Things (IIoT) systems, particularly manufacturing environments. We focused on improving the operational efficiency of a factory floor IIoT system that could suffer from high and unbalanced energy consumption due to the nature of the network deployment. Such behavior is undesirable as it not only increases the carbon footprint of the plant, but also makes the planned maintenance of IoT devices for battery replacement a huge challenge. We propose a heuristic and opportunistic link selection algorithm, HOLA, which not only reduces the overall energy consumption of the IoT network but also balances it across the network. HOLA achieves this energy-efficiency by opportunistically offloading the IoT device data to smart-devices being carried by the workforce in the factory settings. Further, these smart-devices with multiple radio links such as Bluetooth, Wi-Fi, and 3G/4G LTE heuristically determine the best link to transmit the data to the Cloud based on the quality and energy cost of the link. Our experimental and simulation studies validate that HOLA can improve the energy efficiency of IIoT systems by reducing the overall energy consumption and balancing it across the network.

7.2 Future Directions

The current steady adoption of IoT systems and their applications is rapidly fueling, and fulfilling the prediction of having over 50 billion Internet connected devices by the year 2020 [117]. Connecting this huge number of devices to the Internet is a challenging

problem to solve. It will lead to several interesting and important scientific discoveries and contributions not only in Computer Networking, but also in diverse technical and non-technical disciplines of study, due to the inherent interdisciplinary nature of IoT applications. However, all these diverse areas of research will be challenged by two key issues.

First, securing these devices without compromising their usability and performance will be a huge challenge. The ever evolving nature of security threats and attacks makes it challenging for the researchers to secure any network connected device. The physical and software constraints of the IoT devices further amplifies the extent of these challenges. Security schemes employed by OptAuth and OptLock can effectively combat various evolving security attacks. Using the IDS, and other multi-factor security solutions, researchers can create fast, inexpensive, reliable and easy-to-use security mechanisms. However, it should be noted that with IoT systems, it is important to integrate the security mechanisms from grounds up rather than as an afterthought. Without effective security mechanisms in place, IoT would rapidly disintegrate from being “Internet of Things” to being “Internet of Targets”.

Second, connecting these huge number of IoT devices to the Internet efficiently while providing reliable and appropriately fast network connectivity based on the IoT application will be challenging. Overreliance on standard RF technologies could overwhelm them to the point of degradation of service at the very least, and cause adverse effects on human health and inter-device interference at the worst. It will be important to diversify the network connectivity with usage of frequencies across the

electromagnetic spectrum with direct communication techniques at the edge IoT nodes - all without compromising the security. The use of diverse direct and connection-oriented techniques presented in this dissertation - such as use of optical wireless communication, stuffing relevant information in RF beacons, and switching wireless modalities by sampling real-time network performance will be critical to accommodate networking requirements of the projected tens of billion objects in the near future.

REFERENCES

[1] J. Manyika, “The Internet Of Things: Mapping The Value Beyond The Hype,” McKinsey Global Institute, 2015.

[2] L. Da Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, 2014, 10(4), 2233-2243.

[3] K. Dhondge, B. Y. Choi, S. Song, and H. Park, “Optical Wireless Authentication for Smart Devices Using an Onboard Ambient Light Sensor,” In Computer Communication and Networks (ICCCN), 2014 23rd International Conference on (pp. 1-8). IEEE.

[4] K. Dhondge, S. Song, B. Y. Choi, and H. Park, “WiFiHonk: Smartphone-Based Beacon Stuffed WiFi Car2X-Communication System for Vulnerable Road User Safety,” In Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th (pp. 1-5). IEEE.

[5] K. Dhondge, H. Park, B. Y. Choi, and S. Song, “ECOPS: Energy-Efficient Collaborative Opportunistic Positioning for Heterogeneous Mobile Devices,” Journal of Computer Networks and Communications, 2013.

[6] K. Dhondge, R. Shorey, and J. Tew, “HOLA: Heuristic and Opportunistic Link Selection Algorithm for Energy Efficiency in Industrial Internet of Things (IIoT) Systems,” In 2016 8th International Conference on Communication Systems and Networks (COMSNETS), 2016, (pp. 1-6). IEEE.

[7] K. Dhondge, B. Y. Choi, and S. Song, “OptLock: Optical Wireless (Un)locking for Smart Door Locks Using Smartphones,” In The Eighth Central Area Networking and Security Workshop (CANSec Fall 2015), 2015.

[8] “Kill the Password: Why a String of Characters Cant Protect Us Anymore,” Wired, www.wired.com/gadgetlab/2012/11/ff-mat-honanpassword-hacker/all/, 2012.

[9] “Here’s How Knock Code Works on the New LG G Pro 2,” http://www.android central.com/heres-how-knock-code-works-newlg-g-pro-2.

[10] C. Nickle, T. Wirtl, and C. Busch, “Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm,” in Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012, pp. 16–20.

[11] C. Stein, C. Nickel, and C. Busch, “Fingerphoto Recognition with Smartphone Cameras,” in Proceedings of International Conference of the Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–12.

[12] T. Vu, A. Ashok, A. Baid, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, and J. Walling, “Demo: User Identification and Authentication with Capacitive Touch Communication,” in Proceedings of International Conference on Mobile Systems, Applications, and Services, 2012.

[13] F. Zhang, A. Kondoro, and S. Muftic, “Location-Based Authentication and Authorization Using Smart Phones,” in Proceedings of International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 1285–1292.

[14] H. Bojinov and D. Boneh, “Mobile Token-Based Authentication on a Budget,” in Proceedings of Workshop on Mobile Computing Systems and Applications (HotMobile), 2011, pp. 14–19.

[15] “cDs Photoconductive Cells,” http://www.agspecinfo.com/pdfs/G/GL5549.PDF.

[16] S. S. E. T. Specification, “Book 3: Formal protocol definition,” SET Secure Electronic Transaction LLC, Version, 1997.

[17] “AndroSensor,” http://fivasim.pcriot.com/androsensor.html, 2012.

[18] “ATmega328P - Atmel,” http://www.atmel.com/devices/atmega328p.aspx, 2014.

[19] “Arduino Uno Revision 3,” http://arduino.cc/en/Main/arduinoBoardUno, 2014.

[20] “EMC Corporation: RSA SecureID Hardware Authenticators,” http://www.emc.com/security/rsa-securid/rsa-securid-hardwareauthenticators.htm.

[21] “VASCO: Single Button DIGIPASS Devices,” http://www.vasco.com/products/clientproducts/singlebutton digipass/singlebuttondigipass.aspx.

[22] “ISO 20473:2007: Optics and photonics – Spectral bands,” http://www.iso.org/iso/catalogue detail.htm?csnumber=39482.

[23] “Texas Instruments: Revised Pulsoximeter Design Using the MSP430,” http://www.ti.com/lit/an/slaa458/slaa458.pdf, pp. 10–11, 2010.

[24] “Maxell Corporation of America: Button Battery Cross Reference Guide,” http://www.maxell-usa.com/getpdf.aspx?id=34&type=support.

[25] K. Cheng and A. Kumar, “Contactless Finger Knuckle Identification Using Smartphones,” in Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–6.

[26] T. Feng, Z. Liu, K. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, “Continuous Mobile Authentication Using Touchscreen Gestures,” in IEEE Conference on Technologies for Homeland Security (HST), 2012.

[27] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, “Senguard: Passive User Identification on Smartphones Using Multiple Sensors,” in IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2011, pp. 141–148.

[28] T. Kuseler and I. Lami, “Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones,” International Journal of Computer Science and Security (IJCSS), vol. 6, no. 2, pp. 277–287, 2012.

[29] C. Lin, D. Liang, C. Chang, and C. Yang, “A New Non-Intrusive Authentication Method Based on the Orientation Sensor for Smartphone Users,” in IEEE Sixth International Conference on Software Security and Reliability (SERE), 2012, pp. 245–252.

[30] H. Takamizawa and N. Tanaka, “Authentication System Using Location Information on iPad or Smartphone,” International Journal of Computer Theory and Engineering, vol. 4, no. 2, pp. 153–157, 2012.

[31] K. Shin, J. Park, J. Lee, and J. Park, “Design and Implementation of Improved Authentication System for Android Smartphone Users,” in 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012, pp. 704–707.

[32] “Sticky keys: Wireless Proximity Devices,” http://www.stickytec.com/our-products.aspx.

[33] R. Rijswijk and J. Dijk, “Tiqr: A Novel Take on Two-Factor Authentication,” in Proceedings of International Conference on Large Installation System Administration (LISA USENIX), 2011.

[34] G. Alpar, L. Batina, and R. Verdult, “Using NFC Phones for Proving Credentials,” Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance, pp. 317–330, 2012.

[35] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. Choudhury, “Tapprints: Your Finger Taps Have Fingerprints,” in Proceedings of 10th International Conference on Mobile Systems, Applications, and Services (MobiSys), 2012, pp. 323–336.

[36] R. Lichenstein, D. Smith, J. Ambrose, and L. Moody, “Headphone use and pedestrian injury and death in the United States: 20042011,” Injury Prevention, vol. 18, pp. 287–290, 2012.

[37] “GM Developing Wireless Pedestrian Detection Technology,” http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2012/Jul/0726 pedestrian.html, 2012.

[38] “Honda Demonstrates Advanced Vehicle-to-Pedestrian and Vehicle-to-Motorcycle Safety Technologies,” http://www.honda.com/newsandviews/article.aspx?id=7352-en, 2013.

[39] S. Engel, C. Kratzsch, and K. David, “Car2Pedestrian-Communication: Protection of Vulnerable Road Users Using Smartphones,” in Advanced Microsystems for Automotive Applications, pp. 31-41, 2013.

[40] “Wi-Fi Direct,” http://developer.android.com/guide/topics/ connectivity/wifip2p.html.

[41] “German In-Depth Accident Study,” http://www.gidas.org, 2011.

[42] J. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

[43] J. Dulmage, M. Tsai, M. Fitz, and B. Daneshrad, “COTS-based DSRC Testbed for Rapid Algorithm Development, Implementation, and Test,” http://cores.ee.ucla.edu/images/e/ef/Wintech poster Dulmage06.pdf.

[44] R. Chandra, J. Padhye, L. Ravindranath, and A. Wolman, “Beacon-Stuffing: Wi-Fi without Associations,” in Eighth IEEE Workshop on Mobile Computing Systems and Applications, HotMobile 2007, 2007, pp. 53–57.

[45] “Android 2.2 Platform Highlights - Portable hotspot,” http://developer.android.com/sdk/android-2.2-highlights.html.

[46] T. Rappaport, “Wireless Communications Principles and Practice,” Prentice Hall, 1996.

[47] J. White, C. Thompson, H. Turner, B. Dougherty, and D. Schmidt, "WreckWatch: Automatic Traffic Accident Detection and Notification with Smartphones," Mobile Networks and Applications, vol. 16, no. 3, pp. 285–303, 2011.

[48] C. Thompson, J. White, B. Dougherty, A. Albright, and D. Schmidt, "Using Smartphones to Detect Car Accidents and Provide Situational Awareness to Emergency Responders," Mobile Wireless Middleware, Operating Systems, and Applications, vol. 48, pp. 29–42, 2010.

[49] C. Manasseh, Y. Fallah, R. Sengupta, and J. Misener, "Using Smartphones to Enable Situation Awareness on Highways," in ITS America 20th Annual Meeting and Exposition, 2010.

[50] J. Zaldivar, Y. Calafate, J. Cano, and P. Manzoni, "Providing Accident Detection in Vehicular Networks Through OBD-II Devices and Android Based Smartphones," in IEEE 36th Conference on Local Computer Networks (LCN), 2011.

[51] T. Wang, G. Cardone, A. Corradi, L. Torresani, and A. Campbell, "WalkSafe: A Pedestrian Safety App for Mobile Phone Users Who Walk and Talk While Crossing," in Proceedings of the Twelfth Workshop on Mobile Computing Systems and Applications, Hotmobile, 2012.

[52] E. Kwon, S. Song, D. Seo, and I. Jung, "Agent-Based On-Line Traffic Condition and Information Analysis System for Wireless V2I Communication," in Proceedings of the 2nd International Conference on Ubiquitous and Future Networks (ICUFN '10), pp. 360–365, Jeju Island, Republic of Korea, June 2010.

[53] “Global Positioning System Standard Positioning Service Performance Standard,” http://www.gps.gov/technical/ps/2008-SPSperformance-standard.pdf.

[54] “Skyhook wireless,” http://www.skyhookwireless.com/.

[55] E. Trevisani and A. Vitaletti, “Cell-ID Location Technique, Limits and Benefits: An Experimental Study,” in 6th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA ’04), pp. 51–60, December 2004.

[56] “Google Latitude,” 2012, http://www.google.com/latitude.

[57] “Foursquare,” https://foursquare.com/.

[58] U. Bareth and A. Kupper, “Energy-Efficient Position Tracking in Proactive Location-Based Services for Smartphone Environments,” in Proceedings of the 35th IEEE Annual Computer Software and Applications Conference (COMPSAC ’11), pp. 516–521, Munich, Germany, July 2011.

[59] J. Paek, J.Kim, and R.Govindan, “Energy-Efficient Rate-Adaptive GPS-Based Positioning for Smartphones,” in Proceedings of the 8th Annual International Conference on Mobile Systems, Applications and Services (MobiSys ’10), pp. 299–314, New York, NY, USA, June 2010.

[60] “Android 2.2 Platform Highlights—Portable Hotspot,” http:// developer.android.com/about/versions/android-2.2-highlights.html.

[61] “Wi-Fi Direct,” http://developer.android.com/guide/topics/wireless/wifip2p.html.

[62] Y. Zhang, L. Yang, and J. Chen, “RFID and Sensor Networks: Architectures, Protocols, Security and Integrations,” CRC Press, New York, NY, USA, 2009.

[63] T. Rappaport, “Wireless Communications Principles and Practice,” Prentice Hall, New York, NY, USA, 1999.

[64] “3-Axis Geomagnetic Sensor for Electronic Compass,” http://developer. android.com/guide/topics/connectivity/wifip2p.html.

[65] M.Mohorcic, D. Grace, G. Kandus, and T. Tozer, “Broadband Communications From Aerial Platform Networks,” in Proceedings of the 13th IST Mobile and Wireless Communications Summit, pp. 257–261, 2004.

[66] “LANdroids Robot,” http://www.irobot.com/gi/research/AdvancedPlatforms /LANdroidsRobot, 2012.

[67] “The Air Force Has Its Own Batman,” http://money.cnn.com /video/technology /2012/05/18/t-ts-wpafb-batman.cnnmoney/, 2012.

[68] “U.S. Government, Military to Get Secure Android Phones,” http://www. cnn.com/2012/02/03/tech/mobile/governmentandroid-phones/ index .html, 2012.

[69] National Security Agency (NSA), “Nsa-Grade Security Enhanced Android Source Released,” http://www.androidauthority.com/nsa-grade-security enhanced–andr oid-source-released-45532/, 2012.

[70] “Google Maps Location Based Services,” http://support.google.com/maps /bin/answer.py?hl=en&answer=1725632.

[71] “Apple Location Based Services,” http://www.apple.com/privacy/.

[72] B. N. Schilit, A. LaMarca, G. Borriello et al., “Challenge: Ubiquitous Location-Aware Computing and the “Place Lab” Initiative,” in Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH ’03), pp. 29–35, September 2003.

[73] W. Ho, A. Smailagic, D. P. Siewiorek, and C. Faloutsos, “An Adaptive Two-Phase Approach to WiFi Location Sensing,” in Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops ’06), pp. 452–456, Pisa, Italy, March 2006.

[74] D. Kelly, R. Behant, R. Villingt, and S. McLoone, “Computationally Tractable Location Estimation on WiFi Enabled Mobile Phones,” in Proceedings of the IETIrish Signals and Systems Conference (ISSC), 2009.

[75] K. Chintalapudi, A. P. Iyer, and V. N. Padmanabhan, “Indoor Localization Without the Pain,” in Proceedings of the Mobile Computing and Networking (MobiCom ’10), pp. 173–184, 2010.

[76] “Blackberry Locate Service,” https://developer.blackberry.com/devzone/develop/platform services/platform locate.html.

[77] “Ekahau Real Time Location System (RTLS),” http://www.ekahau.com/products/real-time-location-system/overview.html.

[78] “Cisco AeroScout Location-Based Services Solution,” http://www.cisco.com/web/strategy/docs/manufacturing/Aeroscout-Cisco-Brochure.pdf.

[79] “Broadcom: New Location Architecture With BCM4752,” http://www.broadcom.com/products/features/GNSS.php.

[80] F. Schrooyen, I. Baert, S. Truijen et al., “Real Time Location System Over WiFi in a Healthcare Environment,” Journal on Information Technology in Healthcare, vol. 4, no. 6,pp. 401–416, 2006.

[81] A. Ofstad, E. Nicholas, R. Szcodronski, and R. R. Choudhury, “AAMPL: Accelerometer Augmented Mobile Phone Localization,” in Proceedings of the 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-Less Environments (MELT ’08), pp. 13–18, New York, NY, USA, September 2008.

[82] J. Paek, K. H. Kim, J. P. Singh, and R. Govindan, “Energy Efficient Positioning for Smartphones Using Cell-ID Sequence Matching,” in Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys ’11), pp. 293–306, New York, NY, USA, July 2011.

[83] M. Ibrahim and M. Youssef, “A Hidden Markov Model for Localization Using Low-End GSM Cell Phones,” in IEEE International Conference on Communications (ICC ’11), pp. 1–5, Kyoto, Japan, 2011.

[84] E. Martin, O. Vinyals, G. Friedland, and R. Bajcsy, “Precise Indoor Localization Using Smart Phones,” in Proceedings of the 18th ACM International Conference on Multimedia ACM Multimedia 2010 (MM ’10), pp. 787–790, October 2010.

[85] H. Liu, Y. Guan, J. Yang et al., “Push the Limit of WiFi Based Localization for Smartphones,” in Proceedings of the 18th Annual International Conference on Mobile Computing and Networking (Mobicom ’12), pp. 305–316, 2012.

[86] “Calculating Distance Between Two Points Given Longitude/Latitude,” http:// www.freevbcode.com/ShowCode.asp?ID=5532.

[87] R.W. Sinnott, “Virtues of the Haversine,” Sky and Telescope, vol. 68, no. 2, article 158, 1984.

[88] K. Aamodt, “CC2431 Location Engine,” Application Note AN042 (Rev.1.0), Texas Instruments, pp. 7-8, 2006.

[89] “PowerTutor,” http://ziyang.eecs.umich.edu/projects/powertutor/.

[90] “Industrial Internet Consortium,” http://www.iiconsortium.org/index.htm, 2016.

[91] J. Anderton, “Beware of the Hype Around the Internet of Things,” http://www.engineering.com/AdvancedManufacturing/ArticleID/10617/Beware-the-Hype-Around-the-Internet-of-Things.aspx, 2015.

[92] R. McCormic and D. Hartmann, “Smart Factories Need Smart Machines,” Analog Devices Technical Article, 2015.

[93] “Arduino Uno Revision 3,” http://arduino.cc/en/Main/arduinoBoardUno, 2016.

[94] A. I. Dashchenko, “Reconfigurable Manufacturing Systems and Transformable Factories,” Springer, 2006.

[95] E. Upton and G. Halfacree, “Raspberry Pi user guide,” John Wiley & Sons, 2014.

[96] “TCS Connected Universe Platform,” http://www.tcs.com/SiteCollection Documents/Brochures/TCSConnected-Universe-Platform-1214-1.pdf, 2014.

[97] “Splunk,” www.splunk.com, 2016.

[98] E. Cuervo, A. Balasubramanian, D.-k. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, “Maui: Making Smartphones Last Longer With Code Offload,” In

Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, ACM, pp. 49–62, 2010.

[99] M.-R. Ra, J. Paek, A. B. Sharma, R. Govindan, M. H. Krieger, and M. J. Neely, "Energy-Delay Tradeoffs in Smartphone Applications," in Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services. ACM, pp. 255–270, 2010.

[100] K. Dhondge, R. Shorey, and J. Tew, "HOLA IoT Device: Demo," https://youtu.be/-dzS-oDWor4, 2015.

[101] L. Zhang, B. Tiwana, Z. Qian, Z. Wang, R. P. Dick, Z. M. Mao, and L. Yang, "Accurate Online Power Estimation and Automatic Battery Behavior Based Power Model Generation for Smartphones," in Proceedings of the eighth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, ACM, pp. 105–114, 2010.

[102] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, "On Optimal Scheduling in Duty-Cycled Industrial IoT Applications Using IEEE 802. 15.4 e tsch," Sensors Journal, IEEE, vol. 13, no. 10, pp. 3655–3666, 2013.

[103] F. Wang and J. Liu, "Duty-Cycle-Aware Broadcast in Wireless Sensor Networks," In INFOCOM 2009, IEEE, pp. 468–476, 2009.

[104] R. C. Carrano, D. Passos, L. Magalhaes, and C. V. Albuquerque, "Survey and Taxonomy of Duty Cycling Mechanisms in Wireless Sensor Networks," Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 181–194, 2014.

[105] M. Kovatsch, S. Duquennoy, and A. Dunkels, “A Low-Power Coap for Contiki,” in Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on. IEEE, pp. 855–860, 2011.

[106] A. K. Bashir, S.-J. Lim, C. S. Hussain, and M.-S. Park, “Energy Efficient In-Network RFID Data Filtering Scheme in Wireless Sensor Networks,” Sensors, vol. 11, no. 7, pp. 7004–7021, 2011.

[107] L. Wang, L. Da Xu, Z. Bi, and Y. Xu, “Data Cleaning for RFID and WSN Integration,” Industrial Informatics, IEEE Transactions on, vol. 10, no. 1, pp. 408–418, 2014.

[108] C. Konstantopoulos, G. Pantziou, D. Gavalas, A. Mpitziopoulos, and B. Mamalis, “A Rendezvous-Based Approach Enabling Energy-Efficient Sensory Data Collection With Mobile Sinks,” Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 5, pp. 809–817, 2012.

[109] Y. Qu, K. Xu, J. Liu, and W. Chen, “Toward a Practical Energy Conservation Mechanism With Assistance of Resourceful Mules,” Internet of Things Journal, IEEE, vol. 2, no. 2, pp. 145–158, 2015.

[110] P. Baker, and D. Benny, “The Complete Guide to Physical Security.” CRC Press, 2012.

[111] T. Kim, H. Park, S. H. Hong, and Y. Chung, “Integrated System of Face Recognition and Sound Localization for a Smart Door Phone,” IEEE Transactions on consumer Electronics, 59(3), pp. 598-603, 2013.

[112] “Man, It’s Still So Easy to Fool Facial Recognition Software”, Gizmodo, http://gizmodo.com/man-its-still-so-easy-to-fool-facial-recognition-secur-1692220368, 2015.

[113] G. Mone, "Intelligent Living." Communications of the ACM, Volume 57 Issue 12, December, 2014.

[114] “August Smart Lock,” http://www.august.com, 2015.

[115] “Sesame Door Lock,” http://www.candyhouse.co/, 2015.

[116] H. Roland, "Software Card Emulation in NFC-Enabled Mobile Phones: Great Advantage or Security Nightmare." Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU 2012), 2012.

[117] “Behind The Numbers: Growth in the Internet of Things,” https://www.ncta.com/platform/broadband-internet/behind-the-numbers-growth-in-the-internet-of-things-2/, 2015.

[118] “Study of Cognition, Adolescents and Mobile Phones – The Electromagnetic Spectrum,” http://www.scampstudy.org/the-science/#51f8b6924552de7d1d0df5573848424e_one, 2015.

VITA

Kaustubh Dhondge received his Master of Science (MS) in Computer Science in 2011 from University of Missouri – Kansas City (UMKC) with a thesis supervised by Dr. Baek-Young Choi. After receiving his MS, Kaustubh joined the doctoral program at UMKC under the supervision of Dr. Choi. Kaustubh's research interests lie in the areas of mobile systems and applications which involve Internet of Things (IoT), Smart Wearable Systems, Visible Light Communication, Authentication and Security for Smart Devices, Vehicular Communication with Smart Devices, and Positioning & Localization for Smart Devices.

During his doctoral student career, Kaustubh has been fortunate to work alongside some of the best and world renowned researchers at UMKC and TCS Innovation Labs. Together, their research has been published at premier venues, has been recognized with multiple awards, and featured in international technology magazines and news reports.

During the course of his Ph.D. studies, Kaustubh has been awarded the Outstanding Poster Presentation Awards at the Great Plain Network (GPN) conference consecutively in 2011, 2012, and 2013.He was awarded as the Fellow of the University of Missouri System Graduate Student Leadership Development Program (GSLDP) for the 2013-2014 year. He received the Best Video Award at MobiSys 2014. He received the Best Poster Award at the CANSec Workshop held in 2014 and 2015. He was awarded a Research Grant Award by the UMKC School of Graduate Studies for the year 2014-2015 amounting to $6750. Kaustubh has been awarded competitive travel grant awards to several premier conferences including HotMobile, MobiSys, CANSec, and GENI. He was also awarded a

member to the Upsilon Pi Epsilon International Honor Society for Computer Science and Information Technology, and was inducted in 2011.

Kaustubh has enjoyed serving the doctoral and graduate student community at UMKC through various outreach programs and in various capacities at the Graduate Student Council, formerly the Interdisciplinary Doctoral Student Council (IDSC). He served as the President of the IDSC in the 2014-2015 academic year.