IJNRD.ORG ISSN : 2456-4184

International Research Journal
IJNRD
Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# IoT APPLICATIONS: SMARTPHONE COMMUNICATION METHODS

**S. Manikandan**
Assistant Professor, Department of Computer Science, G.F.G.C. K.R. Puram, Bangalore-560036.

## 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).

## 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).

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 significant.

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.

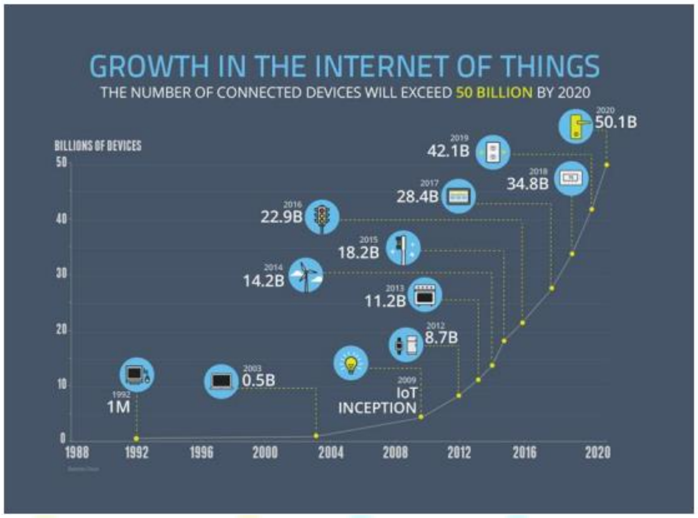

Figure 1. Projected proliferation of the Internet of Things (117).

**Objectives:**

- Optical wireless authentication for smart devices using an onboard ambient light sensor.
- Smartphone based car2x-communication with wifi beacon stuffing for vulnarable road user safety.

**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.

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.

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.

## 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 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.

**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.

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.

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 ~ 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.

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.

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 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.

**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 ~ 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.

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

## 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 38 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

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

## References:

J. Manyika, "The Internet Of Things: Mapping The Value Beyond The Hype," McKinsey Global Institute, 2015.

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.

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.

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

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.

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.

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