IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Internet of Things(IOT) Applications with Diverse Direct Communication method

Astha Shandilya
Mr. Shubham Kumar
4th semester student of M.tech in Computer Science and Information Technology,
MGCU, Motihari.

***Abstract*— The environment around us is heavily populated with intelligent items that are wirelessly connected to one another and eventually to the Internet as our civilization is at a tipping point.The Internet of Things (IOT) idea is based on a network of physical objects or things that are embedded with electronics, software, sensors, and Internet connectivity allowing them to collect and exchange data.**

I. INTRODUCTION

IoT systems and their applications have recently experienced exceptional growth in popularity. According to a recent research, the economic effect of IoT systems will rise from the current 3.9*trillionannuallyto*11.1 trillion by 2025 [1]. The fact that more than 50 billion devices are connected to the Internet is the direct cause of this tremendous economic impact. Connecting commonly used human-use objects to the Internet is one aspect of this growth. The potential for developing such Internet of Things.The number of (IoT) devices available is tremendous. People can engage with machines in a variety of ways using IoT devices.Communication via radio frequency, such as Wi-Fi, Bluetooth, and cellular data connectivity, is at the heart of modern IoT technology. Our reliance on radio frequency communication is growing as connected gadgets become more common. However, the electromagnetic spectrum's radio spectrum, which is incredibly constrained, is becoming less reliable. Other issues include radio frequency pollution, which can be hazardous to human health at high frequencies and interferes with wireless communications.The impact of the radio spectrum constraint will be substantial and could end up being an industry Achille heel as IoT devices proliferate in our homes, workplaces, and other sectors as a rapidly growing number of customers adopt these technologies. We contend that it is critical to vary wireless communication techniques. In this research, we provide completely new, cutting-edge, and complementary wireless communication technologies, such as radio frequency ,infrared and Thought the IOT applications we have created and constructed with those,we may use infrared (IR) and visible lights. In addition to increasing the energy-efficiency,speed, and accuracy of communication, clever, opportunistic, and cooperative use of radio frequency spectrum frequencies and frequencies from the electromagnetic spectrum in general,such as visible light and infrared radiation can also enable novel applications that would not have been possible with existing RF technologies.We throughly examine, evaluate, and contrast their advantages and disadvantages from a range of angles using simulations and experiments, and we offer suggestions for a more interconnected society. Our research contributions in this dissertation are extremely interdisciplinary and span the disciplines of electrical engineering, computer science, and telecommunications and computer networking

II. SMART GADGET OPTICAL WIRELESS AUTHENTICATION WITH AN ONBOARD AMBIENT LIGHT SENSOR

Smartphones are expected to someday operate as the primary devices for a variety of mission-critical jobs that were previously carried out by PCs as their astonishing popularity grows and their software and hardware capabilities advance. Smartphone users will be asked to complete authentication requests just as frequently as PC users because a large share of online services demand various types of client and serve authentications in addition to the access of the cell phones themselves.However, customers find it difficult to use the conventional user id and password entered authentication technique whenever access to the device and the services are required due to the smartphone's small screen and keyboard. Users who are physically challenged or in harsh environments may find it particularly challenging. For instance, government organizations like DARPA,ARL,and NSA have been actively looking for smartphone technology to serve several DoD mission-critical operations, such as the tactical combat mission,disaster recovery, and other mission areas in addition to civilian use. People with problems with fine motor skills or soldiers on the battlefield conducting covert surveillance missions might not be able to quickly put in the correct passcode. Furthermore, there is rising support among theThe following four categories can be used to group authentication techniques: Something a user is aware of (user-know): This includes methods like pin codes, passwords, and pattern that can be The following are things that a user is: This includes physically distinctive characteristics of a person, such as their fingerprints, face ,and iris as well as aspects of their environment, such as their position and orientation.An action taken by a user (user-do):This is an activity that only one individual can produce, example their voice, gesture, and writing signature.Somethings possessed by a user(user-have): This is an exclusive hardware token that is safe that only the owner has access to.There are still problems with security, speed, reliability, and usability despite the

fact that several smartphone authentication techniques has been created to optimize speed and usability while being secure and dependable. For instance, LG debuted Knock Code at the 2014 Mobile World Congress, which unlocks a phone with a knocking motion.The security level is the same as the original pattern-based authentication, despite the usability improvements. Different biometric strategies have been put forth, mostly as a second method of authentication to increase security. The use of biometric-based authentication methods, however, can be computationally. Once their security has been breached, they become expensive and difficult to replace. When a soldier is wearing camouflage or the setting is gloomy, camera-based facial recognition may not be effective. Modern sensor-based authentication methods make use of magnetic, locational, directional, and token-adjacency data. However, circumstances like noise and signal jamming can compromise the accuracy of those authentication mechanisms. The energy consumption of communication sensors like WiFi and Bluetooth is often higher and their negotiation times are longer.

A. CAR2X-COMMUNICATIONS USING SMARTPHONES AND WI-FI BEACONS FOR THE SAFETY OF VULNERABLE ROAD USERS

Vulnerable road users (VRUs) are becoming more and more distracted by activities performed on their smart devices while walking or riding a bicycle on the road, such as watching movies, listening to music, or making phone calls.They are more likely to be involved in street accidents involving vehicles.According to a recent investigation, for instance, ”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.”Althogh many VRU safety infrastructures, like as traffic lights,warning signs, and alert sensors,are set up on the roads to lower the danger of collisions, none of these devices can directly alert distracted VRUs in accordance with the circumstances.A direct alert from vehicles to VRUs still significantly relies on the conventional sound warning approach, even though much of pedestrain safety in intelligent system is oriented towards notifying drivers of the vehicle using the pedestrain detection sensors and nighttime infraed cameras. However, as a result of their smart technologies, more and more VRUs are turning off exterior safety-related warning sounds.As a result, it is crucial to develop a two-way communication system between automobiles and VRU smart devices that can instantly exchange individualized alerts to either side and suggest quick solutions to avoid impending collisions. The researchers create an ad hoc network between the smart gadgets in the vehicles and those carried by VRUs using the WiFi Direct functionality of Android powered devices. They claim that because only the WiFi Direct [40] association time has a latency of about 1 second, it is easy to communicate threats to VRUs. However, it will significantly reduce the coverage distance between the devices in real-world circumstances. In GIDAS [41], [39], for instance, approximately 90all Accidents happen at speeds of up to 60km/h (15 m/s). However, the device is only capable of handling speeds under 25 km/h. Smartphones and tablets are among the smart mobile devices that are quickly taking over our life. They have sparked a paradigm shift away from conventional, constrained phone application and toward intelligent mobile services that are situation-, location-, and context-aware. For instance,a social network-based traffic information system enables every mobile user to report and use both historical traffic information from thes US Department of Transportation and real-time traffic information. As many of those application services require positional data, smart mobile devices provide a variety of positioning services via the Cell-ID Positioning, WiFi-based positioning system, or Global Positioning System. Location-based services (LBSs) rely on GPS, a specialized positioning technology that is made available for many smart devices as an add-on feature. GPS are thought to be the most dependable and well-liked method. However, TTFF, or Time To First Fix makes its high energy usage a significant drawback.WPS calculates a position using database-stored location information from a nearby wireless access point (AP). It utilizes substantially less energy than GPS and has a moderate level of accuracy

B. COOPERATIVE OPPORTUNISTIC ENERGY-EFFICIENT POSITIONING FOR HETEROGENEOUS SMART DEVICES

The Industrial Internet promises to significantly increase productivity and efficiency throughout the supply chain in the manufacturing process. Future processes are likely to be self-regulating,with intelligent gadgets and machinery that may intervene to prevent unanticipated equipment failure. Based on real-time data, individual parts will be automatically replenished. The status of every fixed device in the factory will be reported by every handheld digital device, providing mobile access to real-time, actionable information for staff [90]. The location and workload of each worker in the factory will be tracked by wearable pervasive devices, including sensors, which will increase productivity and offer visibility around-the-clock. These are only several. the examples of large-scale industrial internet’s power. IoT technologies and their applications have recently experienced extraordinary growth and popularity inside the Industrial Internet. According to a recent research, the economic effect of IoT systems will rise from the current 3.9*trillionannuallyto*11.1 trillion by 2025[1]. The fact that 50 billion or more gadgets are connected going online is the direct cause of this tremendous economic impact. Connecting commonly used human-use objects to the Internet is one aspect of this growth. The potential for developing such Internet of Things (IoT) devices is enormous. IoT devices provide a number of ways for people to interact with machines. Examples of these applications include the monitoring of a person’s vital signs via wearable technology, home automation, home security, individualized care and products, smart cars, etc. These applications have a great deal of potential, but an even more important IoT feature involves linking industrial machines to the Internet,

to one another, and to the plant's workforce. This viewpoint serves as the Industrial Internet of Things' foundation.

C. ENERGY CONSUMPTION IN THE INDUSTRIAL INTERNET OF THINGS CAN BE REDUCED AND BALANCED.

The Industrial Internet promises to significantly increase productivity and efficiency throughout the supply chain and in the manufacturing process. Future processes are likely to be self-regulating, with intelligent gadgets and machinery that may intervene to prevent unanticipated equipment failure. Based on real-time data, individual parts will be automatically replenished. In the plant, every handheld digital device will transmit the status of every fixed device, providing staff with mobile access to real-time, useful information. The location and workload of each worker in the factory will be tracked by wearable pervasive devices, including sensors, which will increase productivity and offer visibility around-the-clock. These are only a few instances of the Industrial Internet's immense power. IoT technologies and their applications have recently experienced extraordinary growth and popularity inside the Industrial Internet. According to recent research, the economic effect of IoT systems will rise from the current 3.9*trillionannuallyto*11.1 trillion by 2025[1]. The fact that 50 billion or more gadgets are connected going online is the direct cause of this tremendous economic impact. Connecting commonly used human-use objects to the Internet is one aspect of this growth. The potential for developing such Internet of Things (IoT) devices is enormous.IoT devices provide a number of ways for people to interact with machines. Examples of these applications include the monitoring of a person's vital signs via wearable technology, home automation, home security, individualized care and products, smart cars, etc. These applications have a great deal of potential, but an even more important IoT feature involves linking industrial machines to the Internet, to one another, and to the plant's workforce. This viewpoint serves as the Industrial Internet of Things' foundation

D. Dissertation Outline

The dissertation's remaining sections are organized as follows. We outline a novel token-based authentication method for smartphones and other smart devices. Many smartphone users foresee conducting numerous mission-critical tasks on their smartphones that were previously carried out by utilizing PCs as recent smartphone advancements in software and hardware keep on developing. Smartphone authentication has thus emerged as one of the most important security concerns.Traditional user id and password typed authentication is viewed as an inconvenient and time-consuming solution because of the comparatively small form factor of smartphones. Alternative authentication techniques like pattern, gesture, finger print, and facial recognition have been actively investigated,using unfair means of the numerous sensor capabilities of smartphones. However, the speed, dependability, and usability of authentication systems continue to be a problem. They are especially unsuitable for individuals who face physical challenges and harsh environments. This dissertation chapter's evaluation of alternative smartphone authentication methods To suggest authenticating using ambient light sensors for cell phones in a variety of usage circumstances. A programmable Fast, Inexpensive, Reliable, and Easy-to-use (FIRE) hardware authentication token has been devised and prototyped by our team. The smartphone that receives and decodes the Optical Wireless Signal (OWS) sent by the FIRE token's inbuilt LED to send passwords employs the smartphone's ambient light sensor. We created the Inverse Dual Signature (IDS) to enable multi-factor authentication for essential smartphone applications, and the FIRE token is a component of the challenge-response method. Together, they offer the smartphone user Optical Wireless Authentication (OptAuth). Our tests demonstrate that OptAuth can authenticate a user on a smartphone in a straightforward, quick, and reliable manner without jeopardizing security. the user experience and security level [3]. We explain our investigation on vehicular or vehicle communications in this dissertation to reduce pedestrian-car collisions. Vulnerable road users (VRUs) are becoming more and more distracted by smartphone-related activities while walking or riding a bike on the road, such as watching movies, listening to music, or making calls. The protection of such VRUs from automobiles still significantly relies on conventional sound warning systems, despite the development of different high-tech Car-to-Car(C2C) and Car-to-Infrastructure(C2I) connections to improve traffic safety. Additionally, as smartphone adoption spreads widely, VRUs are becoming less aware of warning sounds related to safety..According to a study on traffic accidents, there have been 300involving VRUs wearing headphones in the past ten years. Nevertheless, recently a few

III. CONCLUSION

Various automakers have proposed car-pedestrian communication techniques, but their practical use is limited since they often call for specialized communication equipment to handle the wide range of mobility and also assume that VRUs will actively pay attention to the conversation while walking. In this chapter of the dissertation, we suggest a Car2X communication system based on smartphones called WiFi-Honk that can warn of impending crashes to both VRUs and automobiles in order to protect the distracted VRUs in particular. Without the need for a specific gadget, WiFi-Hong offers a useful safety method for the distracted VRUs utilizing a smartphone.When whether in WiFi Direct or Hotspot mode, Wifi-Honk eliminates the WiFi associated overhead by using beacon-stuffed WiFi communication with the smartphone's position, speed, and direction information replacing its SSID. It also offers a reliable WiFi hotspot.collision estimation algorithm to send out the proper alerts. Our simulation and experimental investigations demonstrate that WiFi-Honk can successfully inform VRUs with enough time for a response, even in highly mobile situations

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. Communication" *3rd IEEE Workshop on Optical Wireless Communications (OWC'12)*, pp. 1244-1248.

[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

International Research Journal
IJNRD
Research Through Innovation