Blue-tooth Low Energy Based Vehicle Access Solutions: Insights,Challenges and Trends

Prachi Shah *,Minda Corporation Limited,Pune*
Suresh D*, Minda Corporation Limited, Pune*
Prashant v. Joshi*, Reva University Banglore*
Sudarshan KM*, Reva University Banglore*

---***---

Abstract -Automotive technology is rapidly moving towards attaining more and more connectivity related and autonomous features. Since first interaction of a vehicle user with the vehicle is in the form of accessing/entering the vehicle, it has been on of the major comfort/convenience/security features supported by electronics. As BLE (Bluetooth Low Energy) communication technology is entering aggressively in many industrial application, automotive technology is no exception. Vehicle access technology is also gradually migrating towards use of BLE based smart-phone enhancing customer convenience and security. This paper discusses automotive application requirements of vehicle access solutions highlighting increasing role of BLE technology. Various system design issues like reliable communication and security related aspects covering possible relay attacks and their counter-measures are discussed. Upcoming trends using BLE 5.0 technology so as to enhance communication range at reduced power is also touched upon. Role of BLE 5.0 supporting IOT (Internet of Things) is highlighted to understand directions automotive applications are pursuing in this regard. The paper is intended to equip automotive system designers with a survey of necessary insights into technical and system aspect of this technology focused around vehicle access application. Such insights would be valuable for charting upcoming system technology road-map for automotive applications.

1.INTRODUCTION

Electronics has been penetrating our lives in general and vehicle is particular for past several decades. As vehicles play an increasing role in our life, it is becoming customary that people expect their vehicle to be a home away from the home. As our lives are increasingly woven around high-tech gadgets like smart-phones, vehicles too need to be increasingly be controlled through smart-phone. Blue tooth Low Energy (BLE) has become a preferred choice for smart-phone based in vehicle control of various features. The driving factor behind the same are motivated by the desire to facilitate vehicle users to use their Bluetooth low energy-equipped smartphones and portable devices to manage applications revolving around in-vehicle control, personalized infotainment, vehicle diagnostics, car access, vehicle sharing and piloted parking. As the industry also evolves to be greener, replacing cables using low-power wireless technology is another major potential for Bluetooth low energy. In this paper we dwell upon BLE based vehicle access solutions, the challenges involved, countermeasures and conclude with the insights gained. This paper outlines the necessary BLE fundamentals and system design aspects apart from the state of art technology features for the benefit of the automotive system designers of the vehicle access control systems. This will facilitate them to make right system design decisions. **Section 2** discusses BLE fundamentals while **Section 3** dwells upon BLE based vehicle access requirements and features. **Section 4** considers security considerations for this application, while **Section 5** outlines major relay attack mechanisms as well as their counter-measures based on the state-of-the-art practices. **Section 6** highlights further technology roadmap based on BLE 5 features such as IoT (Internet for the Things) support and range enhancement. **Section 7** sums-up the paper consolidating the insights discussed

2.0BLE Fundamentals

Bluetooth emerged as a technology for replacing the cables with a wireless link for a short distance. The early application during 1990s centered around wireless links among PC or a Personal Digital Assistant (PDA) ,mouse, keyboard etc. Bluetooth operates over 2.4GHz ISM (Industrial, Scientific and Medical) band BLE was introduce much later in 2010 as a low energy variant. It was intended for low duty cycle applications such as IoT (Internet of Things). BLE is the right solution where data communication is required with low duty cycles and data throughput requirements are relatively moderate. As the name suggests it consumes less power and hence preferred for automotive applications like smart key- based vehicle access, diagnostics, actuation of mirrors, seats etc. in line with pre-programmed parameters tailored for the authenticated vehicle user [1] [2]

For the home user and commercial business 2.4 GHz is the primary band one uses for WiFi, Bluetooth, cordless phone, printer, keyboard, mouse and gaming controller applications. Voice, video and data communications are typically used in 2.4 GHz systems requiring higher data rates (up to 300 Mbps for 802.11n applications) [3]

3.0BLE Based Vehicle Access Requirements Features. [3]

Automotive applications for smart phone operated features need to meet requirements below:

- Low power, Low cost, low complexity and low bandwidth operation
- Worldwide available unlicensed frequency band
- High security, a robust wireless link and a strong industry ecosystem.

3.1 Low Power, Low complexity and Low Bandwidth

Automotive electronic devices enhance vehicle features but also tend to consume energy eating into fuel consumption of the vehicle. Some of the electronic units need to be consuming a minimal amount of power in "sleep" mode [1] so that they can be "woken-up at will even when the vehicle is ignition is off and the vehicle is in the parked condition. "Smart Key" based vehicle application do require such a feature.

Bluetooth low energy is tailored from the physical layer (PHY) to higher operational layers to keep power consumption to a minimum. At the PHY, Bluetooth low energy specifies relatively relaxed channel spacing (2 MHz) and selectivity requirements, and uses the constant-envelope Gaussian frequency shift keying (GFSK) modulation scheme, which allows the use of power-efficient nonlinear power amplifier designs. Bluetooth lowenergy specifies only 37 channels and performs discovery on three channels. Discovery and connection times can be kept as low as a few milliseconds given this simple channelization scheme.

Low power consumption at the network protocol layer is achieved by efficient duty cycled operation (allowing the device to stay connected in sleep mode and briefly waking up to transmit a small amount of data), together with strict power management and low transmission overhead. These relaxed requirements allowsemiconductor vendors to optimize sleep and active currents and shorten switching times. These optimizations enable (single mode) BLE devices to be simple, low power and low cost.

3.2 Worldwide Availability of a Non-licensed Band

ISM (Industrial, Scientific and Medical) frequency band is used by BLE at 2.4 GHz. For automotive applications across the globe this eliminates the intensive effort required for licensing and retuning the circuits to the licensee band available in various countries.

3.3 High Security

Protecting a consumers' private information is important for every wireless system; for automotive applications, security is of paramount importance. Secure communications keep exchanged data safe and at the same time prevent unauthorized devices from injecting data to trigger unintended operation of an automotive system.

The Bluetooth low energy toolbox supports fivebasic security services:

•**Pairing and bonding** to create one or more shared secret keys and store those keys for usein subsequent secure connections.

•**Authentication** to verify the identity of communicating Bluetooth low energy-enabled devices based on their address.

•**Confidentiality** to prevent information compromise caused by eavesdropping, and ensure that only authorized devices can access and understand exchanged data.

•**Authorization** to allow the control of resources and ensure that a device is authorized to use a service before permitting it to do so.

•**Message integrity** to verify that data exchanged between two Bluetooth low energy devices has not been altered or compromised in transit.

3.4 Reliable Wireless Link

The achievable RF link budget and co-existence with other wireless systems are the main determining factors governing the robustness and reliability of a wireless connection. The achievable Bluetooth low energy range is inherently governed by the factors below:

- Maximum transmission power
- Antenna performance
- Obstacles in the communication path

To improve transmission robustness, Bluetooth low energy employs the adaptive frequency hopping (AFH) scheme common to all flavours of Bluetooth to minimize interference from other wireless technologies in the 2.4-GHz ISM band. Bluetooth low energy can for instance dynamically update the frequency-hopping sequence to avoid channels where interference occurs during active communications. Frequency hopping is also a power-efficient way to mitigate multipath fading issues. From an RF perspective, Bluetooth low energytechnology is capable of satisfying the required performance for automotive applications.

3.5 Passive Entry Passive Start (PEPS) Application Using BLE

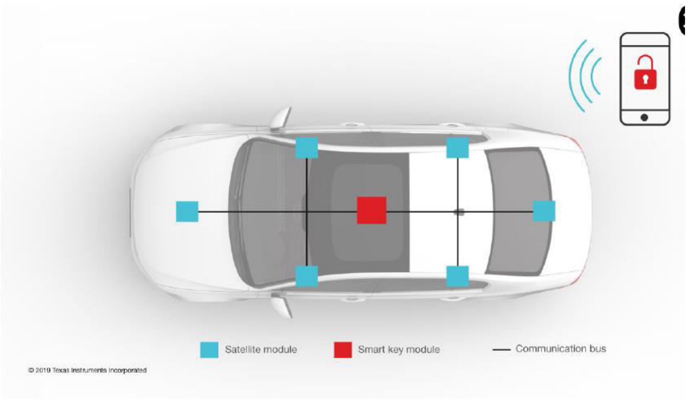

Fig. 1:A passive-entry passive-start architecture in a car. The number of satellite modules will vary, depending on system-level requirements

Fig 1 shows BLE based PEPS system. A smartphone or other smart device is used by the vehicle user to authenticate himself. BLE link is established through secure pairing (as explained in the subsequent sections) with the vehicle control unit responsible for vehicle access control. After due authentication the vehicle control unit obeys the user commands for locking/unlocking doors, starting the vehicles etc. Position of the smart phone inside the vehicle is securely detected by the satellite units distributed across the vehicle interior.

This allows the vehicle control unit to securely detect the presence of the smart phone inside the vehicle and allow the authenticated vehicle user to start the vehicle. Also, these satellite nodes allow the vehicle user approaching the vehicle from different sides of the car. Vehicle start command is honored only if the smart phone is located within the vehicle. The satellite units help the system to localize the user position.

4.0 Security Considerations for Smart Key Based Vehicle Access

4.1 Trust Establishment through Pairing and key generation/exchange

The pairing mechanism is the process where the devices involved in a communication exchange their identity information to establish trust and get the encryption keys ready for future data exchange. The four options for pairing, included in Bluetooth 4.2 and later revisions, are just works, passkey entry, out of band (OOB) and numeric comparison. Bluetooth core specification version 4.2 introduced the Federal Information Processing Standard (FIPS)- compliant elliptical curve Hellman-Diffie (ECDH) algorithm for key exchange. This was a great security enhancement to the pairing process.

4.2 Encryption. Encryption in Bluetooth low energy uses the Advanced Encryption Standard (AES) in the Counter Mode with Cipher Block Chaining Message Authentication Code protocol. This function generates 128-bit encrypted data from 128-bit key and 128-bit plain-text data using the AES 128-bit block cypher as defined in FIPS 197.

4.3 Signed data. Bluetooth low energy supports the ability to send authenticated data over an unencrypted channel between two devices with a trusted relationship. The transmitter first signs the data packets with a secure signature comprising a message authentication code generated by the signing algorithm and a counter (to protect against a replay attack). Upon reception, if the receiver verifies the signature, the data is presumably from a trusted source.

4.4 Privacy. Bluetooth low energy supports a feature that reduces the ability to track a Bluetooth low energy device over a period of time by changing the device address frequently. Only trusted devices can resolve this private address.

5.0 Possible Relay Attacks and counter measures [4].[5],[6]

5.1 Various Prevalent Relay Attacks: Many possible relay attacks have been widely documented in the literature [4],[5]. We will consider here two major types of attacks relevant for vehicle access application:

- Passive Eaves-dropping attack
- Man- In-The-Middle Attack

Both the attacks and their counter measures are discussed in detail in subsequent sections

5.2 Passive Eaves-dropping Attack and Measures to Arrest the Same

For our application towards vehicle access, this involves secretly snooping upon the communication privately so as to replicate the same for accessing a vehicle with malicious intent. In other words, Passive eavesdropping is the process by which a third device listens in to the data being exchanged between the two paired devices. Bluetooth low energy secure Connections uses the ECDH public key cryptography to combat passive eavesdropping attacks. The ECDH algorithm provides a very strong mechanism when exchanging keys over an unsecured channel and makes it extremely difficult for a malicious device to guess the encryption key.

Key to creating formidable entry barriers for an Eaves-dropping attacker lies in strengthening the "key exchange" phase of BLE pairing sequence. BLE 4.0 and 4.1 rely on temporary kay (TK) or short term key (STK) based exchange. These strategies are vulnerable to eves-dropping attacks. On the other hand BLE 4.2 employs

what are known as LE Secure Connections. Instead of using a TK and STK, LE Secure Connections use a single Long Term Key (LTK) to encrypt the connection. This LTK is exchanged/generated using Elliptic Curve Diffie Hellman (ECDH) public key cryptography which offers significantly stronger security compared to the original BLE key exchange protocol (4.0 and 4.1)

5.3 Man In the Middle (MITM) Attack

In an MITM attack, as two Bluetooth low energy devices (such as a car and a smartphone virtual key) try to communicate with each other, a third device inserts itself between them and emulates each device to the other. Authentication through secure pairing or signed data can protect against MITM attacks and ensure that a vehicle is communicating with the intended virtual key and not an unauthorized attacker. It is possible to efficiently integrate Bluetooth low energy security features on single-mode Bluetooth low energy ICs.

For example, state of art Bluetooth low energy wireless MCUs [10] support all Bluetooth 4.2 and 5.0 security features. They include a highly efficient AES encryption hardware module, a cryptography library in read-only memory (ROM) (elliptic curve), a true random number generator (TRNG) and related security signal processing. These features are effective tools that can enable automotive designers to implement Bluetooth low energy security and other customized security solutions for their applications. Bluetooth low energy technology provides several features to cover the encryption, trust, data integrity and privacy of user data in and around a connected car. Automotive OEMs, Tier 1s and third-party developers can achieve secure and reliable wireless communication through the use of these security features and other innovative techniques.

Reference [7] lists additional counter measures against the relay attack as below:

- Use of a motion sensor, which shuts off BLE response from a smart phone/BLE key fob if the same is not under motion, thus effectively ignoring the communication from the attacker
- Use of a pair barometer to ensure that the height of the BLE smart device is same as height of the vehicle. The vehicle transmits its height during its communication to the authentic BLE device. Hence the authentic smart BLE device refuses to respond if the vehicle height does not match the device height. Hence if BLE smart device is kept on a work table which would be much above the ground level of the parking lot, a relay attacker cannot communicate with the same
- Another ultimately secure strategy consists of power modulation during communication between the smart device and vehicle. Different communication frames are transmitted between the vehicle and the smart devise is a sequence of predefined but secret sequence of power levels. This amounts to resorting to a secret amplitude modulation of the signal strength to counter a relay attack. A communication is honoured as authentic only when it is able to demodulate the power-sequence and verify that it is in line with the prescribe secret pattern. An attacker cannot mimic the same and hence fails to carry the attack

6.0 Upcoming Trends for Using BLE in Automotive[8]

As Blue-tooth 5.0 enhances BLE specifications to include IOT features as well as range enhancements by the factor 4. With IOT enabled Bluetooth link this technology can play a key role in autonomous and connected vehicle. One interesting fallout of this can be absence of traffic signals. The vehicles will self-coordinate the traffic around intersections reducing the traffic jams.

BLE 5.0 enhances range by using redundant bits in the communication. By sending 8 symbols per bit we can enhance the range needed for "remote vehicle finding feature "available with simple 433 Mhz remote key less entry system. But with limited range of BLE 4.2 the same can only be done from a limited range of around 20meters. With BLE 5.0 we can have arrange of 80 meters approximately (at the cost of reduced baud-rate of 0.125 MBPs)

BLE 5.2 makes it possible for devices to dynamically optimize the transmission power through a dynamic trade-off between optimally needed received signal strength and transmission power. The receivers actively monitor the received signal strength. In case of excess RSSI (received signal strength) the receivers communicate the host to to reduce the transmission power. The Bluetooth controller can also monitor and report path loss changes to the Bluetooth host using the concept of zones, which some application types will find useful. This also results in improved reliability of the communication link[13]

7.0 Conclusion.

This paper discusses and consolidates the important aspects of BLE based vehicle access solutions. Useful BLE features which meet the automotive requirements are outlined. Various challenges like security and range limitations are discussed. Counter measures for opposing relay attacks based various technology-based measures are highlighted. BLE 5.9 based new features are analyzed for their upcoming applications for vehicle access as well as trends towards connected/autonomous solutions. The paper should serve as a sound knowledge resource for the automotive system engineers to make right technology and system decisions for architecting state of art vehicle access solutions.

REFERENCES

1. Khanh Tuan Le, Systems Engineer, Texas Instruments Bluetooth Low Energy and the automotive transformation, https://www.ti.com/lit/wp/sway008/sway008.pdf?ts=1621656745134&ref_url=https%253A%252F%252Fwww.google.com%252F
2. The Basics of Bluetooth Low Energy (BLE) By Mohammad Afaneh | May 6, 201

   https://www.novelbits.io/basics-bluetooth-low-energy/
3. By Dan Torres, Texas Instruments, Exploring Bluetooth: Exploring connectivity trends for Bluetooth Lowapplications Low Energy in automotive applications, June 15.2020

   https://www.electronicproducts.com/exploring-connectivity-trends-for-bluetooth-low-energy-in-automotive-applications/
4. Mathew Bo, A Basic Introduction to BLE 4.x Security, Oct 2016

   https://forum.digikey.com/t/a-basic-introduction-to-ble-4-x-security/12501
5. AnsafIbrahemAlrabady and Syed MasudMahmud,Some Attacks Against Vehicles' Passive Entry Security Systems and Their SolutionsIEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 52, NO. 2, MARCH 2003 431
6. Aur´elienFrancillon, Boris Danev, SrdjanCapkun, , Relay Attacks on Passive Keyless Entry andStart Systems in Modern Cars

   https://eprint.iacr.org/2010/332.pdf
7. US Patent US 2018/0186332 A1 July 5,2018
8. SamnthaMorhead, How to Pick the Best Bluetooth Protocol for Your Application, July 19th 2016, Electronic Design