Mitigating Relay Attacks in Vehicle Access Systems Using BLE and UWB

D. Suresh
School of Electronics and Communication Engineering, REVA University, Bangalore, India
sureshd@mindacorporation.com

Prashant V. Joshi
School of Electronics and Communication Engineering, REVA University, Bangalore, India
prashantvjoshi@reva.edu.in (corresponding author)

Parag Parandkar
Lead IPR Cell, SPARK MINDA Technical Center, MINDA Corporation Limited, India
parag.parandkar@mindacorporation.com

Received: 5 June 2025 | Revised: 11 July 2025 | Accepted: 20 July 2025

 DOI: https://doi.org/10.48084/etasr.12581

ABSTRACT

The technology for accessing vehicles has evolved significantly from traditional mechanical keys to advanced keyless systems, utilizing smartphones and smart wearables. The conventional LF-RF-based Passive Entry and Passive Start (PEPS) systems, struggle with inherent vulnerabilities. In particular, they suffer from relay attacks that exploit signal amplification to bypass proximity detection mechanisms. As vehicles become more connected through V2X and other shared mobility ecosystems, securing access systems is more critical than ever. To address these challenges, this research proposes a secured vehicle access framework that combines Bluetooth Low Energy (BLE), Ultra-Wideband (UWB), and Near Field Communication (NFC). Our system introduces multi-layered defense mechanisms, including asymmetric encryption-based digital key applets, dynamic Unique Rolling Session Keys (URSKs), and UWB-based secure ranging, using Time Difference of Arrival (TDOA) and trilateration techniques for precise user localization. BLE is used exclusively for authenticating the legitimate device. Passive unlocking is permitted only after proximity is verified by UWB, ensuring that the user's device is truly near the vehicle. The development process utilized ANSYS HFSS 3D High Frequency Simulation for dual antenna design which enabled precise calibration. The implementation was achieved using a chipset with an ARM Cortex M33 core with hardware accelerators. Our experiments demonstrated that the system reliably triggers door unlock within only a 1.6 m radius, thus effectively mitigating relay attack risks. This framework offers a robust, future-ready, and user-centric solution for next-generation vehicle access control.

Keywords-relay attack prevention; Passive Entry Passive Start (PEPS); Bluetooth Low Energy (BLE); Near Field Communication (NFC); Time of Flight (ToF); Ultra Wide Band (UWB)

I. INTRODUCTION

Modern vehicles use various electronic systems alongside traditional mechanical keys for entry and ignition control. The vehicle's Electronic Control Unit (ECU) emits a Low-Frequency (LF) signal (~125 KHz) when the door handle is activated. The owner's key (Fob), upon receiving this LF signal, responds with a high-frequency (RF) signal (315/433 MHz) [1]. The ECU authenticates the RF response and unlocks the doors within milliseconds. This LF-RF exchange also controls engine start via a push button. This forms the Passive Entry Passive Start (PEPS) system, enabling keyless access and engine ignition when the Fob key is nearby without manual input [2]. The vehicle triggers the LF signal on door latch activation; the Fob key replies with an RF signal, and upon verification, access is granted. Figure 1 illustrates the PEPS access control system. PEPS rely on measuring proximity using the Received Signal Strength Indicator (RSSI), which estimates the Fob key's distance based on signal strength. The presence of multiple antennas determines whether the key is inside or outside the vehicle. However, RSSI-based systems are vulnerable to relay attacks as the attackers usually extend the signal range to trick the vehicle into unlocking [3]. While RSSI does not require time synchronization, relayed messages increase delay thus risking unauthorized access [4]. Despite that PEPS offer convenience, its security depends on robust measures against relay attacks.

Calculating the Time of Flight (ToF) can estimate the distance between the Fob key and the vehicle. If the ToF value

exceeds a predefined time threshold, the Fob key is out of the vehicle's range. To manipulate ToF-based distance estimation, an intruder must receive, interpret, reconstruct, and retransmit the signal, which poses significant challenges [5].

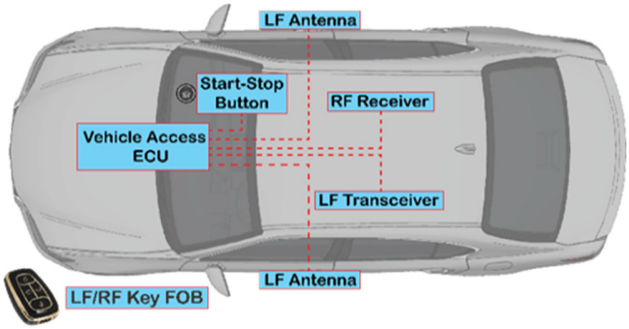

Fig. 1. Access Control System using PEPS.

A. Relay Atttack

PEPS is a type of vehicle security system that automatically unlocks doors and enables engine start via a push button when an authorized key is detected nearby. These systems operate through a challenge-response authentication mechanism using LF and RF signals. The vehicle's ECU broadcasts LF signals containing identification data through in-vehicle antennas and awakes the Fob key from low-power mode [6]. Once the fob decodes the LF transmission, it sends an encrypted RF message by using a pre-shared secret key that the ECU verifies before granting access. A symmetric encryption, typically AES-128, secures this exchange by offering a large key space that resists brute-force attacks [7]. However, PEPS remains vulnerable to relay station attacks, where adversaries deploy two transceivers to extend the communication range as shown in Figure 2. To mitigate relay attacks, the usual countermeasures include measuring the RSSI, distance-bounding algorithms, and time-difference methods. These measures help ensure that the Fob is within a legitimate proximity before granting access [8-11]. Equation (1) depicts the distance calculation using Round Trip Time (RTT) where t_n depicts the processing time at the target and c is the speed of light.

$$d = c \cdot \frac{(RTT - t_n)}{2} \quad (1)$$

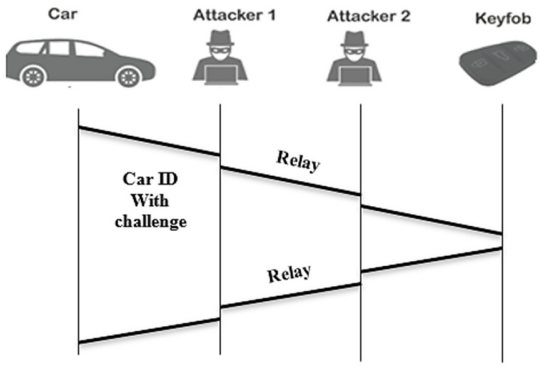

Fig. 2. Relay attack on conventional PEPS system.

B. Alternative Vehicle Access Techniques – BLE, UWB, and NFC

Bluetooth Low Energy (BLE) is a popular choice for long-range, keyless, and smartphone-based vehicle access due to its ability to support functions like owner pairing, digital key operations, remote commands, and notifications. It can detect a driver's presence beyond 10 m and also enables preparation for Ultra-Wideband (UWB) authentication by estimating the distance using signal strength and data packets [12].

BLE incorporates security mechanisms such as 128-bit AES encryption in CCM mode, a true random number generator, and periodic device address changes, to ensure privacy and resist detection. It has compact size, low power usage, and supports methods like PEPS. These assets make it cost-effective for automotive applications [13]. UWB, based on the IEEE 802.15.4z standard, combats distance manipulation by transmitting over a wide frequency band. It uses short pulses for high-speed data transmission and precise measurements of Angle-of-Arrival (AoA) and ToF. It also uses Scrambled Timestamp Sequence (STS) encryption to protect timestamp data, thus preventing relay attacks and allowing centimeter-level distance accuracy.

Near Field Communication (NFC) serves as a backup when BLE is unavailable by authenticating access through a passive tag embedded in the phone or the Fob. Finally, UWB complements BLE by activating only when BLE fails thus enhancing system security [14-18].

C. Key Technical Aspects and Technology Comparison

The Key Technical aspects of BLE, UWB and NFC are shown in Table I:

TABLE I. KEY TECHNICAL ASPECTS OF BLE, UWB, NFC

Parameter	BLE	UWB	NFC
Accuracy	1-5 m	± 10 cm	5 cm
Reliability	Sensitive to multipath and interference	Resilient to multipath and interference	No multipath
Range	25 m – 100 m	70 m – 250 m	< 1 m
Date Rate	2 Mbps	27 Mbps	424 Kbps
Latency	Typ > 3 s	Typ < 1 ms	Typ < 1 s
Security	Sensitive to relay attack and jamming	Non-sensitive to relay attack and jamming, supports STS	Non-sensitive to relay attack because of close proximity communication
Tracking accuracy	Medium	High	High
Data Security	High	High	Low

The identified research gaps are:

- Relay Attack Vulnerability: Current BLE-based PEPS systems rely on signal strength which makes them susceptible to relay attacks [19].
- Intermittent UWB Ranging: UWB is accurate but often not continuously active. It allows potential security lapses [20].
- Weak Session Management: Existing systems lack dynamic and secure session keys to prevent replay and key reuse attacks [21].

- Limited Multi-Technology Integration: Effective combination of BLE, UWB, and NFC for seamless, secure, and fail-safe vehicle access is underdeveloped [22].

The key contributions of the proposed work are:

1. A secure authentication mechanism is designed using BLE for initiation and UWB for precise proximity detection.
2. Relay attack resistance is enhanced with Ultra-Resilient Secure Keying (URSK) and secure channel establishment protocols.
3. A hybrid BLE-UWB system for continuous secure proximity tracking with accurate distance and angle estimation is developed.
4. Context-aware access control features like lock/unlock and engine start-stop based on UWB-based location tracking are implemented.

II. THE PROPOSED SOLUTION

A. *System Architecture of PEPS*

The PEPS system architecture ensures secure and efficient vehicle access through hardware and server-based components, as depicted in Figure 3. The vehicle connects to the Vehicle Manufacturer Server via a Telematics link (1) controlled by the manufacturer. It includes NFC readers and optional BLE or UWB modules for owner pairing and vehicle access functions. Engine start is managed via NFC links (3, 4) or BLE/UWB links (11, 12). The owner's mobile device communicates with the Owner Device OEM Server and Vehicle OEM Server via a proprietary method (2) and an app interface (10). A friend's device can similarly access the Vehicle OEM Server using a proprietary app interface (9). The owner and friend devices manage the Digital Key applet lifecycle, including certificate updates via links (2) or (7) and can suspend, restore, or wipe digital keys if a device is lost or stolen.

The Vehicle OEM Server handles user accounts, identification and verification, and may also connect to an optional Key Tracking Server (5) that registers issued Digital Keys securely while maintaining user data privacy. Security is ensured by a Secure Element (SE) embedded in both the mobile device and the ECU Vehicle Access. This SE is an automotive-grade secure microcontroller, resistant to electrical and physical attacks and suitably equipped with cryptographic accelerators. It supports secure storage of keys and data and enables multiple authentication methods [23].

The Vehicle Access ECU (SE) and mobile device will pair by using a Digital Key applet, which performs key creation, encryption, pairing, secure ranging, key sharing, and vehicle access operations. The UWB module maintains a secure level comparable to the NFC interface through secure ranging, thus protecting it against relay attacks. The Vehicle Access ECU and mobile device use a URSK to initiate and terminate ranging sessions. These keys are derived from the Digital Key authentication handshake and stored securely within the ECU and phone. To mitigate potential security risks, these keys have a limited lifetime of one hour or less, reducing the time window for an attacker [24].

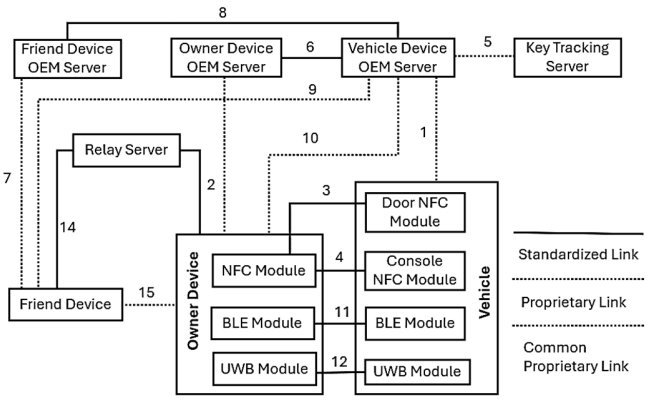

Fig. 3. System Architecture of PEPS.

III. IMPLEMENTATION

The UWB ranging method was initially implemented using the Time Difference of Arrival (TDOA) technique. Additionally, trilateration techniques were employed to accurately determine the phone and user location coordinates, including distance and AoA, from the Vehicle Access ECU [25]. The compiler and debugger tool chain were specifically selected by the semiconductor supplier. The ARM Cortex M33 core chipset is used with hardware accelerators and BLE stack through an SDK (Software Development Kit). This implementation was carried out using the chipset in automotive vehicle access devices, a BLE key fob and a BLE Electronic Handle Lock.

A. *Trilateration Calculations*

Out of the four distances obtained from the anchors, the three shortest distances are selected. Trilateration is performed using the chosen three anchors, each having coordinates (X1, Y1), (X2, Y2), and (X3, Y3). The intersection point (X, Y) derived from these coordinates indicates the location of the UWB tag. This method ensures accurate positioning as illustrated in Figure 4.

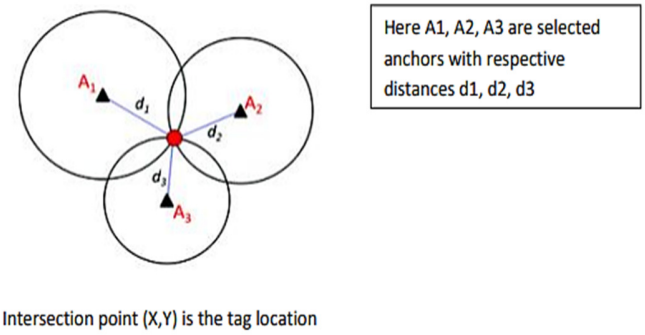

Fig. 4. Trilateration Technique.

Using the standard distance formula, we get:

$$(X - x1)^2 + (Y - y1)^2 = d1^2 \quad (2)$$

$$(X - x2)^2 + (Y - y2)^2 = d2^2 \quad (3)$$

$$(X - x3)^2 + (Y - y3)^2 = d3^2 \quad (4)$$

On solving (2), (3) and (4), we get, (5) and (6):

$$(-2 \cdot x1 + 2 \cdot x2) \cdot X + (-2 \cdot y1 + 2 \cdot y2) \cdot Y = (d1)^2 - (d2)^2 - (x1)^2 + (x2)^{2-} - (y1)^2 + (y2)^2$$

$$(-2 \cdot x2 + 2 \cdot x3) \cdot X + (-2 \cdot y2 + 2 \cdot y3) \cdot Y = (d2)^2 - (d3)^2 - (x2)^2 + (x3)^{2-} - (y2)^2 + (y3)^2$$

$$A \cdot X + B \cdot Y = C$$

$$D \cdot X + E \cdot Y = F$$

$$X = (CE - FB)/(EA - BD) \quad (5)$$

$$Y = (CD - AF)/(BD - AE) \quad (6)$$

B. UWB Ranging and Localization Zones

Key ranging and localization experiments have been conducted by utilizing UWB secure ranging techniques. The vehicle access ECU ensures secure ranging. All measurements were recorded. The BLE RSSI values and UWB signal strength of the Key FOB/Mobile Device are measured by the Vehicle Access ECU at various angles, ranging from 0° to 360°, relative to the vehicle's position. The following important preconditions were set:

- Successful authentications are done for the right Mobile device (after pairing) using the DK applets residing in SE Element.
- URSK authentication has been done over BLE (Dynamic Secret KEY).
- UWB sessions are triggered by BLE RSSI in the ECU.
- The Lock Threshold is <= 1.6 m.
- Unlock Threshold >= 0.5 m.
- No care zone: 0.5 to 1.6 m.
- Threshold values are calibrated based on actual business requirements.
- UWB values are calibrated for the distance values in each direction.

The key results presented below demonstrate the signal values of the Fob key and the Vehicle Door lock-unlock status concerning the established threshold values.

C. Results and Discussion

Accurate ranging using UWB technology is performed by the vehicle's ECU access to make secure lock/unlock decisions. A region vulnerable to relay attacks exists because the UWB ranging is inactive. BLE communication remains active and triggers UWB when in proximity, typically within a 2 m range, whereas the ECU initiates secure ranging and unlocks the doors. UWB measurements within this range validate the effectiveness of the ranging mechanism. Table II shows the BLE RSSI and UWB signal measurements for vehicle access control at various angles and distances. It also depicts the lock and unlock status at 1.6 m and 0.5 m respectively.This study reveals that BLE RSSI and UWB ranging values for lock and unlock operations vary across different angular positions and distances. At 0.5 m, UWB values fall within lower bounds, while BLE RSSI values remain higher, enabling unlock functionality. At distances beyond 1.6 m, UWB values increase significantly, while BLE RSSI drops below -80 dBm and triggers lock function. This validates the effectiveness of combining BLE RSSI and UWB measurements for secure, accurate, and context-aware vehicle access control.

Our work emphasizes the significance of antenna placement and line-of-sight in real-world scenarios, to ensure robust performance under various approach vectors. The BLE-UWB system effectively addresses security assumptions by considering adversaries capable of relay and spoofing attacks. It ensures robust proximity detection and authentication. Its threat model accounts for both passive and active attacks. It also incorporates countermeasures like URSK and secure channel establishment, to mitigate vulnerabilities in wireless communication.

Table III compares some existing works [26-28] with the proposed study. It is proven that they lack real-time proximity checks, secure distance estimation, and practical deployment. The use of vulnerable RF Fob keys can be seen in [26]. UWB without implementation is discussed in [28]. The proposed work overcomes these gaps with BLE-triggered UWB ranging, RSSI-based authentication, and URSK-based cryptography. This enables secure access, accurate localization, and strong relay attack resistance for modern keyless entry systems.

TABLE II. BLE RSSI AND UWB SIGNAL MEASUREMENTS FOR VEHICLE ACCESS CONTROL AT VARIOUS ANGLES AND DISTANCES

Angle (º)	Mobile distance from car (m)	BLE RSSI low & high values	UWB low & high values	Lock (1.6 m)	Unlock (0.5 m)
0º (Front Side)	1	-72 to -85	372 to 389	NO	YES
0º (Front Side)	2	-72 to -88	480 to 491	YES	NO
0º (Front Side)	3	-79 to -91	584 to 608	YES	NO
0º (Front Side)	4	-75 to -93	687 to 746	YES	NO
0º (Front Side)	5	-78 to -94	820 to 846	YES	NO
45º (Front Right)	1	-72 to -80	362 to 366	NO	YES
45º (Front Right)	2	-74 to -88	480 to 490	YES	NO
45º (Front Right)	3	-75 to -85	597 to 646	YES	NO
45º (Front Right)	4	-76 to -90	705 to 726	YES	NO
45º (Front Right)	5	-81 to -94	824 to 840	YES	NO
90º (Right Side)	1	-54 to -72	227 to 239	NO	YES
90º (Right Side)	2	-68 to -84	323 to 346	YES	NO
90º (Right Side)	3	-71 to -88	430 to 451	YES	NO

90º (Right Side)	4	-68 to -87	535 to 556	YES	NO
90º (Right Side)	5	-68 to -83	642 to 672	YES	NO
135º (Right Back)	1	-66 to -83	321 to 354	NO	YES
135º (Right Back)	2	-66 to -78	428 to 451	YES	NO
135º (Right Back)	3	-80 to -95	464 to 546	YES	NO
135º (Right Back)	4	-74 to -92	581 to 616	YES	NO
135º (Right Back)	5	-77 to -88	644 to 682	YES	NO
180º (Back Side)	1	-63 to -78	299 to 304	NO	YES
180º (Back Side)	2	-68 to -81	318 to 375	YES	NO
180º (Back Side)	3	-73 to -91	490 to 493	YES	NO
180º (Back Side)	4	-78 to -92	567 to 569	YES	NO
180º (Back Side)	5	-81 to -96	666 to 669	YES	NO
225º (Back Left)	1	-69 to -78	319 to 323	NO	YES
225º (Back Left)	2	-70 to -76	408 to 412	YES	NO
225º (Back Left)	3	-69 to -80	510 to 515	YES	NO
225º (Back Left)	4	-72 to -83	614 to 626	YES	NO
225º (Back Left)	5	-69 to -80	793 to 802	YES	NO
270º (Left Side)	1	-52 to -60	230 to 240	NO	YES
270º (Left Side)	2	-62 to -88	346 to 354	YES	NO
270º (Left Side)	3	-65 to -84	429 to 433	YES	NO
270º (Left Side)	4	-66 to -76	509 to 512	YES	NO
270º (Left Side)	5	-73 to -90	619 to 647	YES	NO
315º (Left Front)	1	-68 to -90	397 to 425	NO	YES
315º (Left Front)	2	-73 to -89	497 to 504	YES	NO
315º (Left Front)	3	-77 to -91	638 to 647	YES	NO
315º (Left Front)	4	-79 to -90	752 to 768	YES	NO
315º (Left Front)	5	-75 to -96	868 to 874	YES	NO

TABLE III. COMPARISON WITH EXISTING WORKS

Parameter	**[26]**	**[27]**	**[28]**	**Proposed**
Authentication mechanism	Vulnerable to replay attacks using RF relay systems	Proposes multi-factor authentication combining biometrics and mobile devices	Mentions use of UWB for enhanced security	Uses BLE for initiation and secure UWB ranging for accurate proximity detection
Relay attack resistance	Lacks robust protection against relay attacks	Limited mitigation through multi-factor approach	Suggests UWB is resistant but not detailed	Implements URSK and secure channel establishment to prevent relay attacks
Technology used	RF-based communication with limited encryption	RF + mobile-based biometrics	Survey on UWB technology in telematics	BLE + UWB hybrid system with continuous secure proximity tracking
Ranging accuracy	Not focused on accurate ranging	Does not include ranging mechanisms	Describes UWB potential but no implementation	High-accuracy UWB ranging with distance and angle estimation
Access control features	Manual Fob key use	User validation via biometrics and smartphone	General access control overview	Context-aware access including lock/unlock, engine start-stop based on UWB location

IV. CONCLUSION

This study compared BLE-based RSSI and UWB-based distance estimation techniques for secure vehicle access. The results showed that BLE RSSI provides general proximity detection but lacks precision due to environmental noise and signal variability. UWB technology showed improved accuracy and reliability in determining distance and direction of the mobile device relative to the vehicle.

Our analysis suggests that secure ranging using UWB is a viable approach to mitigate relay attacks in keyless entry systems. The vehicle access ECU uses UWB ranging to authenticate access requests based on accurate spatial measurements. This leads to unlocking the vehicle only when the mobile device is within the verified proximity range. The integration of a secure digital key applet, unique session keys (URSK), and cryptographic authentication, ensures that even sophisticated relay attacks are prevented.

In summary, combining BLE for initial triggering and UWB for precise ranging and secure access in next-generation keyless vehicle entry systems, enhances security without compromising user convenience.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to the SPARK MINDA Technical Centre & School of Electronics and Communication Engineering, REVA University, for their invaluable support and guidance during this research.

REFERENCES

[1] Gyu-Ho Kim, Kwan-Hyung Lee, Shim-Soo Kim, and Min Ju Kim, "Vehicle Relay Attack Avoidance Methods Using RF Signal Strength," *Communications and Network*, vol. 5, no. 3, pp. 573-577, Jan. 2013, https://doi.org/10.4236/cn.2013.53B2103.

[2] A. I. Alrabady and S. M. Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions," in *IEEE Transactions on Vehicular Technology*, vol. 52, no. 2, pp. 431-439, Mar. 2003, https://doi.org/10.1109/TVT.2003.808759.

[3] D. Suresh, P. V. Joshi, P. Parandkar, and K. M. Sudharshan, "An Improved Authentication Scheme for V2I Communication," *SN Computer Science*, vol. 5, no. 5, Art. no. 535, May 2024, https://doi.org/10.1007/s42979-024-02865-7.

[4] D. Moriyama, "Automotive System Security," Automotive Core Technology Development Division, White paper, Renesas, AST-AB-22-0117 Rev.1.0, Oct. 19, 2022.

[5] D. Suresh, P. V. Joshi, P. Parandkar, A. Gambhir, and K. M. Sudharshan, "BLE Channel Sounding: novel method for enhanced ranging accuracy in vehicle access," *IEEE Access*, vol. 13, pp. 67531-67547, Jan. 2025, https://doi.org/10.1109/ACCESS.2025.3561028.

[6] D. Suresh, P. V. Joshi, P. Parandkar, and K. M. Sudharshan, "Intrusion detection in in-vehicle networks using neuro computing," *Proceedings of the International Conference on Innovative Comouting and Communication Data Analytics and Management (ICICC-2024),* Aug. 2024.

[7] A. Kout, B. Bouaita, A. Beghriche, S. Labed, S. Chikhi, and E. B. Bourennane, "A Hybrid Optimization Solution for UAV Network Routing," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10270–10278, Apr. 2023, https://doi.org/10.48084/etasr.5661.

[8] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Securing smart vehicles from relay attacks using machine learning," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 2665–2682, Apr. 2020, https://doi.org/10.1007/s11227-019-03049-4.

[9] C. M. Chen, B. Xiang, Y. Liu, and K. H. Wang, "A secure authentication protocol for Internet of Vehicles, " *IEEE Access*, vol. 7, pp. 12047–12057, Jan. 2019, https://doi.org/10.1109/ACCESS.2019.2891105.

[10] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Secure passive keyless entry and start system using machine learning," in *11th International Conference and Satellite Workshops, SpaCCS 2018, Melbourne, NSW, Australia, Proceedings*, Dec. 2018, https://doi.org/10.1007/978-3-030-05345-1_26.

[11] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654–1667, Oct. 2019, https://doi.org/10.1109/TIFS.2019.2946933.

[12] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "A new hybrid online and offline multi-factor cross-domain authentication method for IoT applications in the automotive industry," *Energies*, vol. 14, no. 21, Art. no. 7437, Nov. 2021, https://doi.org/10.3390/en14217437.

[13] Z. Guo, Y. Zhang, J. Cao, X. Ren, X. Zhao, and H. Li, "Secure multifactor authentication and access control mechanism for electronic bill service in a 5G cloud-fog hybrid architecture," *Security and Communication Networks*, vol. 2022, May 2022, https://doi.org/10.1155/2022/3658402.

[14] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, Art. no. 4954, Jan. 2019, https://doi.org/10.3390/s19224954.

[15] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the security of carrier phase-based ranging," *International Conference on Cryptographic Hardware and Embedded Systems*, Taipei, Taiwan, pp. 490–509, Aug. 2017, https://doi.org/10.1007/978-3-319-66787-4_24.

[16] A. Lacava, V. Zottola, A. Bonaldo, F. Cuomo, and S. Basagni, "Securing Bluetooth Low Energy networking: An overview of security procedures and threats," *Computer Networks*, vol. 211, Art. no. 109021, Jul. 2022, https://doi.org/10.1016/j.comnet.2022.108953.

[17] R. Zhang, L. Song, A. Jaiprakash, T. Talty, A. Alanazi, and A. Alghafis, "Using ultra-wideband technology in vehicles for infrastructure-free localization," in *Proceedings IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, pp. 15–18, Apr. 2019, https://doi.org/10.1109/WF-IoT.2019.8767347.

[18] Staat, Paul, Kai Jansen, Christian Zenger, and Christof Paar, "Securing Phone as a Key Against Relay Attacks," *18th escar Europe,* pp. 48-58, 2020.

[19] Abubaker, Radi "Novel Channel Based Relay Attack Detection Protocols in the Physical-Layer." PhD diss., University of Waterloo, 2024.

[20] Jyothy Anu, and Anie George, "Unlocking the potential: Ultra-Wideband," *i-manager's Journal on Electronics Engineering*, vol. 14, no. 2, pp. 31-39, Jan. 2024, https://doi.org/10.26634/jele.14.2.20357.

[21] Limbasiya, Trupil, Ko Zheng Teng, Sudipta Chattopadhyay, and Jianying Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," *Vehicular Communications*, vol. 37, no. 100515, Oct. 2022, https://doi.org/10.1016/j.vehcom.2022.100515.

[22] J. M. De Guia, J. E. Estrada, G. L. Opina, and A. Tripathi, "Real-time personnel tracking system of operator processes using Bluetooth low energy & camera in warehouse environment," in *Proc. IEEE 14th International Conference Humanoid, Nanotechnol., Inf. Technol., Commun. Control, Environ., Manage. (HNICEM)*, pp. 1–6, Dec. 2022, https://doi.org/10.1109/HNICEM57413.2022.10109532.

[23] Stocker, Michael, Bernhard Großwindhager, Carlo Alberto Boano, and Kay Römer. "Towards secure and scalable UWB-based positioning systems," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, IEEE, pp. 247-255, Dec. 2020, https://doi.org/10.1109/MASS50613.2020.00039.

[24] Vivek, Burri Sri Venkat, Talluri Vineetha, Aaka Teja, Boyapati Sai Keerthana, Dinesh Kumar Anguraj, and Hari Kiran Vege, "Security and Efficiency in Tap and Pay: The Promise and Challenges of BLE and UWB Integration," in *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, pp. 714-722, Oct. 2024, https://doi.org/10.1109/ICOSEC61587.2024.10722236.

[25] DERVİŞOĞLU, İsmail, and Uraz YAVANOĞLU, "Security Threats and Performance Evaluation of Ultra Wideband and Bluetooth Low Energy Technologies for Indoor Positioning," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, IEEE, pp. 22-27, Dec. 2021, https://doi.org/10.1109/ISCTURKEY53027.2021.9654342.

[26] Kapulica, A., Dakić, V., Morić, Z. and Petrunić, R., "Key Fob Replay Attacks on Personal Vehicles: Vulnerabilities and Mitigation Strategies," in *2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, IEEE, pp. 1-5, May 2024, https://doi.org/10.1109/HORA61326.2024.10550523.

[27] D. Brito and S. Abuzneid, "Multi-Factor Authentication for Keyless Entry Systems: An Innovative Approach to Automotive Security," *Journal of Information Security*, vol. 16, no. 1, pp. 78–100, Nov. 2024, https://doi.org/10.4236/jis.2025.161004.

[28] M. Rogobete, M. I. Mihailescu, and E. Marin, "Ultra-Wideband Technology in Telematics Security - A short Survey," in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Pitesti, Romania, pp. 1–6, July 2021, https://doi.org/10.1109/ECAI52376.2021.9515057.