Ultra-Wideband Sensor Network and Deep Learning Technique Based LTE Network for Military Application

Khushbu Meena[1], Rahul Jain

Article History: Received:02-07-2023 Revised:01-08-2023 Accepted:14-08-2023

Abstract

This research presents a comprehensive approach to enhance security in LTE mobile networks using a combination of fingerprint input, encrypted data, and Ultra-Wideband (UWB) carrier aggregation. The primary focus of this work is on developing an attack detection system based on a trained dataset and classifier to safeguard LTE networks against potential threats.The system starts by collecting fingerprint input data from users for authentication purposes. These fingerprints are encrypted using robust encryption algorithms to ensure data confidentiality during transmission and storage. To improve data throughput and network efficiency, UWB carrier aggregation is implemented to enable high-speed data transfer while maintaining low-latency communication. To train the attack detection classifier, a dataset comprising various attack scenarios and normal network behavior is constructed. Deep learning techniques develop a robust classifier capable of identifying and differentiating between legitimate users and potential attackers. The attack detection system continuously monitors network activity and analyzes encrypted data using the trained classifier. If any anomalous behavior is detected, indicating a potential attack, the system triggers appropriate countermeasures and notifies the network administrators.

In this military application, we propose a secure and efficient system that combines fingerprint input, encrypted data transmission, Ultra-Wideband (UWB) technology, carrier aggregation, and an LTE mobile network for attack detection. The system aims to enhance security and prevent unauthorized access to sensitive military facilities.

Keywords: UWB, LTE networks. Security,Transmitter receiver, Deep learning technique

DOI: 10.48047/ecb/2023.12.8.641

[1]PhD Research Scholar , Department of Electronics and Communication Engineering , JECRC University Jaipur, Rajasthan ,India.

[2]Assistant Professor , Department of Electronics and Communication Engineering , JECRC University Jaipur, Rajasthan, India.

Email: khushiprakash1992@gmail.com

1. Introduction

Although the traditional Doppler radars have been commonly applied in perimeter monitoring systems, they will fail to detect the target and create coverage shadows when the protected area has obstacles or in a foliage. Additionally, a large object moving outside of the range of interest can create false alarms because of the limited range resolution of narrow-band radars, which cannot distinguish a nearby small target from another larger longer-range one. With a capability of excellent range resolution and penetration, on the other hand, UWB sensor radars have attached extensive investigations in recent years [1]. The emitted UWB signal occupies a tremendous bandwidth typically of several Gigahertz (GHz). Its fractional bandwidth is also very large, usually greater than 0.2, resulting in a sensor with exceptional resolution that also has the ability to penetrate many common materials. More importantly, such UWB sensors would be independent of Doppler shifts but would detect intrusion by measuring changes in the impulse response of environments.

In [2, 3], UWB through-wall motion sensing radars and UWB ground penetrating radars (GPRs) are introduced to meet the requirements of special war field and the probe and rescue after a natural disaster. Recently, Liang et al. initiated the target detection in foliage using UWB radars and proposed that the log-logistic model was much suitable to represent UWB propagation channel in the foliage [4, 5]. Then, the sense-through-foliage target detection using UWB sensors is investigated in [6–8]. These researches significantly benefit the sense-through-wall and other subsurface sensing problems [9], which has become asymmetric threats in current and future military operational environments.Although the rapid progress in UWB research is originally inspired by radar sensors to a great extent, UWB sensor networks have also been widely recommended for different applications. For example, UWB network is an ideal candidate for shortrange high-data-rate transmission which has been fully 2 EURASIP Journal on Wireless Communications and Networking discussed in the IEEE standard of wireless personal area network (WPAN), owing to its extremely wide bandwidth [10]. The energy efficiency issue in UWB network is also addressed through medium access control (MAC) protocol design in [11]. As the demand of data acquisitions and transmissions in various applications continues to grows, such as environment pollution sensing, intelligent traffic guiding, and remote medical monitoring, the current spectrum has become overcrowded and it is hard to allocate fixed frequency band to these new services. Accordingly, the trend of many networks for different purposes operating in nearby geographical regions seems inevitable. So, the interference mitigation and coexistence issues between UWB sensors and other networks should be carefully addressed. The UWB emission power regulation campaign error, launched by U.S. Federal Communications Commission, has been preceded for some years intending for interference mitigation [12]. However, this simple power control strategy does not seem sufficient for antagonistic cooperation between these networks [13]

The concept of Ultra-Wideband (UWB) technology has been in existence since the late 1950s and has gained acceptance as a wireless technology with exceptional characteristics. UWB systems are also known by various names such as impulse radio, ultra-wideband systems, time modulation systems, baseband systems, among others.

According to the definition provided by the FCC's First Report and Order, UWB signals must have bandwidths greater than 500 MHz or a fractional bandwidth larger than 20 percent at all times of transmission. Fractional bandwidth (FBW) is a measure used to classify signals as narrowband, wideband, or ultra-wideband. It is calculated by taking the ratio of the bandwidth at -10 dB points to the center frequency of the signal, expressed as a percentage. This equation (Equation 1) provides a clear relationship for determining the fractional bandwidth of UWB signals based on their bandwidth at -10 dB points and center frequency. UWB technology's ability to utilize such large bandwidths enables it to provide high data transmission rates, precise localization capabilities, and robust communication and radar systems with various applications across different industries[14-15].

FBW = (BW_10dB / f_c) * 100%

Equation 1: Fractional Bandwidth (FBW)

Where FBW is the fractional bandwidth of the signal (expressed as a percentage).

BW_10dB is the bandwidth of the signal at -10 dB points.

f_c is the center frequency of the signal.

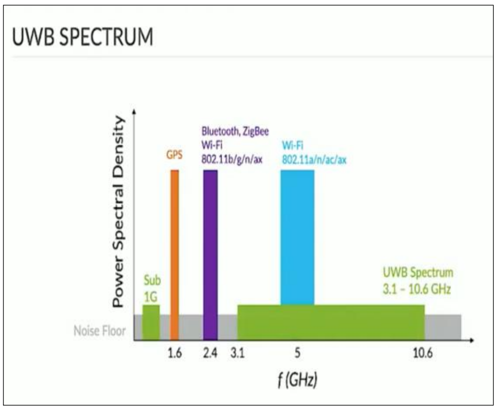

Figure.1 Ultra wide band frequency range

2. Related work

UWB [16], standardized by IEEE 802.15.3, is a data transmission method in a wireless network that offers, as the name suggests, a very large bandwidth. This high-rate throughput capability is really a great support to WBAN considering the number of wearables and sensors are used for remote monitoring these days. But the winning property of UWB that is applicable in WBAN is the significant power efficiency that it provides. The lower energy consumption increases the sensor operational period and life even transmitting more data.

There are two approaches to implement UWB: i) multi-band (MB) OFDM UWB, and ii) impulse radio (IR) UWB [17]. Characteristically, the second one is more suitable for WBAN because IR-UWB radios are generally of low-complexity by design and consume less power. The reason behind that is, to transmit and receive data, IR-UWB systems use pulses of very short duration (typically 2–3 ns) [18]. That is why they are preferable for the WBAN applications which are energy constrained and require short-range communication. In addition to that, the UWB physical layer is designed to provide WBAN robustness and the capability to implement high-performance operations [19].

UWB suffers from an important drawback. To achieve the short pulse width and power efficient signal transmission, the designing of the front-end circuitry of a UWB receiver is somewhat complex and also consume more power [20].

3. Proposed system

An ultra-wideband (UWB) sensor network for military security transmitter and receiver attack detection using deep learning and time-catch attack detection proposes a comprehensive system to enhance military security by detecting attacks on communication systems.

3.1. Attack Detection Algorithm

Collect and preprocess the person fingerprint data to ensure consistency and uniformity. Preprocessing may involve resizing, normalization, and feature extraction from the fingerprint images. Use the trained ResNet-50 model as the basis for detecting attacks. Define the necessary threshold for similarity/dissimilarity between the figure prints of individuals.

Continuously monitor the UWB data from the sensor network to detect individuals in the vicinity. For each individual detected, extract their figure print data (e.g., images). Pass the figure print data through the ResNet-50 model to identify the individual. Compare the identified individual with known authorized individuals in the system. If the identified individual does not match any known authorized individual and exceeds a predefined dissimilarity threshold, raise an alert for a potential unauthorized person or attack.

Ultra-wideband technology allows for the transmission and reception of signals across a wide frequency range. UWB sensor nodes can be strategically deployed throughout a military communication infrastructure to monitor and analyze signals.

3.2. Transmitter and Receiver Attack Detection

The focus of this system is to detect attacks on both transmitters and receivers in the military communication system. Such attacks could include signal jamming, spoofing, unauthorized access, or other forms of interference.

3.3. Time-Catch Attack Detection

Time-catch attack detection involves capturing the timing information of UWB signals to identify potential attacks. Irregularities or deviations in signal arrival times can be indicative of malicious interference. To enhance security against different types of attacks, including time attacks, power attacks, and catch attacks, a comprehensive system can be developed using a combination of techniques and strategies. Below is an overview of how such a system might work.

3.4. Time Attack Detection

Time attacks are aimed at exploiting vulnerabilities related to timing and synchronization in systems. These attacks can include replay attacks, timing side-channel attacks, and more. To detect time attacks.

3.5. Power Attack Detection

Power attacks exploit power consumption patterns of electronic devices to extract sensitive information or disrupt system operations.

3.6. Catch Attack Detection

Catch attacks involve an attacker capturing and replaying legitimate data or signals to deceive the system.

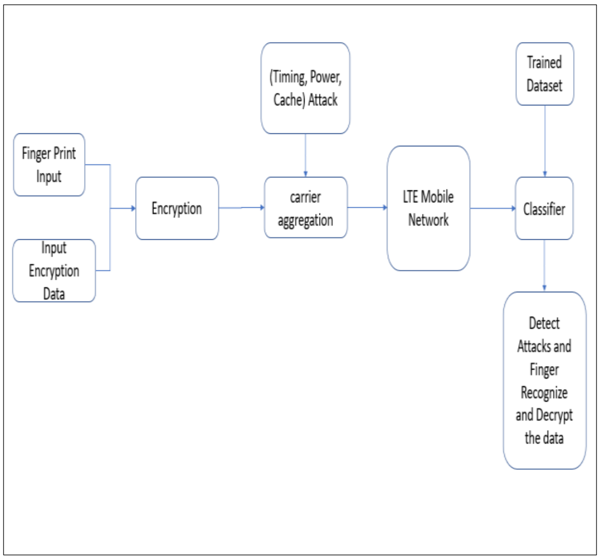

Figure. 2 Flow Diagram

4 Simulation results

To build a system for attack detection in an LTE mobile network using fingerprint input, encrypted data, and carrier aggregation, we need to follow these steps:
The system's core components include:

4.1. Fingerprint Input

Individual authentication is achieved through fingerprint biometrics, providing a reliable and unique identifier for each authorized user.

4.2. Data Encryption To safeguard sensitive information during transmission, data encryption is employed using robust encryption algorithms, ensuring confidentiality and data integrity.

4.3. Ultra-Wideband (UWB) UWB technology is integrated into the system for precise localization, enabling real-time tracking and monitoring of personnel and assets within military facilities.

4.4 Carrier Aggregation The system leverages carrier aggregation in the LTE mobile network to enhance data throughput and network reliability, ensuring seamless and fast

data transmission.

4.5. Training Dataset and Classifier A comprehensive dataset of fingerprint samples is used to train a classifier based on deep learning techniques. The classifier accurately identifies and validates authorized personnel.

4.6. Attack Detection The trained classifier is extended to detect and respond to potential attacks within the military application. Unrecognized fingerprints, abnormal data patterns, or suspicious behaviors trigger security alerts for immediate response and mitigation.

5 Simulation parameters

The system is evaluating the Error Vector Magnitudes (EVM) for different sub-frames and carriers in an LTE network. The simulation measures the RMS of the EVM for all included channels and signals over all symbol-times in the measurement interval. The output also indicates that a timing attack has been detected in the carrier_data-aggregated code, which involves transmitting encrypted finger image data through the LTE network to check for authorized or unauthorized users.The simulation is conducted at a sample rate of 61.4400 Ms/s.

The LTE system uses Carrier Aggregation (CA) with a total bandwidth of 44.6000 MHz, divided into different component carriers (CCs).

The component carriers have center frequencies (Fc) of -16.8000 MHz, -4.8000 MHz, and 12.3000 MHz, respectively.

5.1. EVM Evaluation The simulation measures the EVM at different edges (low and high) for each subframe (subframe 0 to 9) in the LTE system.

- The low edge EVM and high edge EVM are calculated for each subframe, representing the accuracy of received constellation points compared to the ideal ones.

- The averaged EVM values for all sub-frames and edges are provided, with the overall averaged EVM being 0.664%.

5.2. CRC Check

- After decoding the transmitted subframes, a cyclic redundancy check (CRC) is performed to verify the integrity of the received data.
- All subframes (subframe 0 to 9) pass the CRC check, indicating that the received data is error- free.

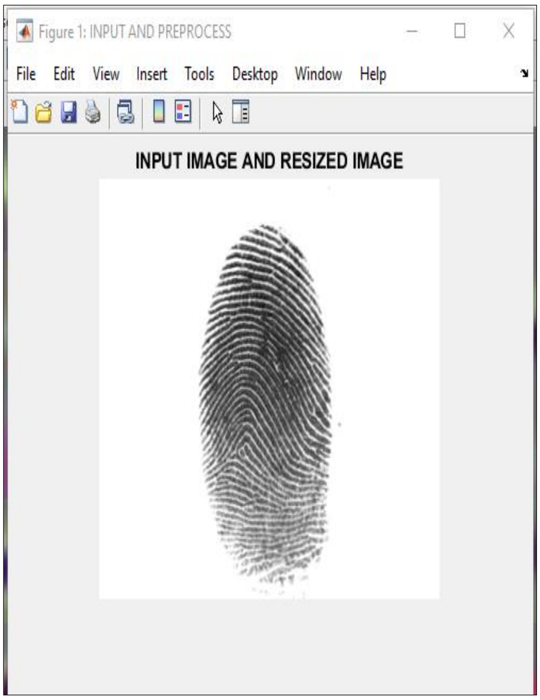

Figure.3 figure print input for authentication

When the individual attempts to access a system or service, they are prompted to provide their fingerprint as input for authentication.

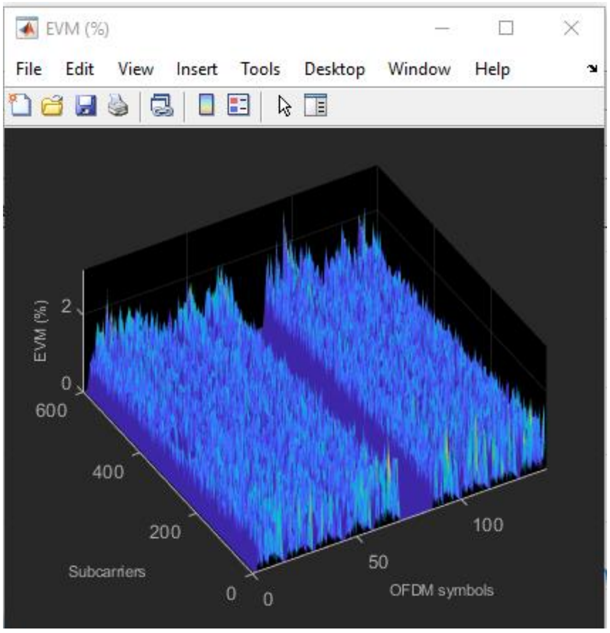

Figure.4 EVM and in-band emissions

A lower EVM value indicates a higher signal quality and more accurate modulation, while a higher EVM value implies more distortion and inaccuracies in the received signal.

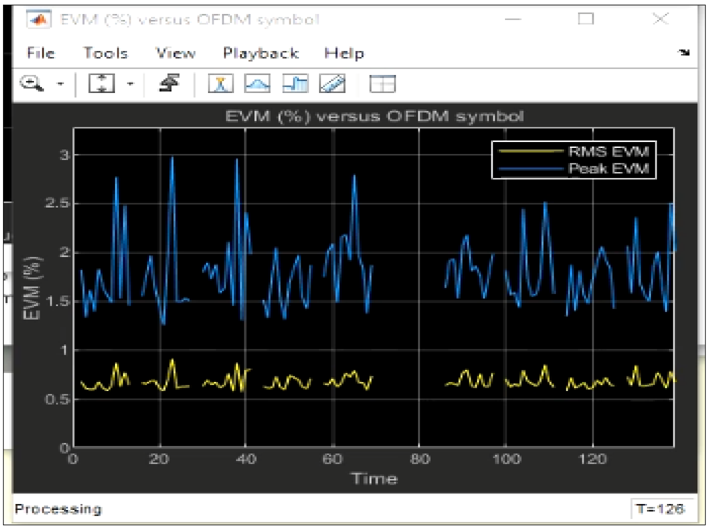

Figure.5 Root Mean Square (RMS) of the Error Vector Magnitudes for all included channels and signals for OFDM

5.3. Measure EVM for Each Channel and Signal

For each channel and signal in the OFDM system, measure the EVM between the received constellation points and the expected ideal constellation points. This involves comparing the I-Q (In-phase and Quadrature) values of the received signal with the expected I-Q values based on the modulation scheme used.

5.4. Calculate EVM for Each Channel and Signal

For each channel and signal, calculate the EVM value using the following formula:

$$\mathbf{EVM = \sqrt{[(I\_error^2 + Q\_error^2) / (I\_expected^2 + Q\_expected^2)]}}$$

Where:

- I_error and Q_error are the error components (difference between received and expected I-Q values).
- I_expected and Q_expected are the expected I-Q values based on the modulation scheme.

- Square and Sum the EVM Values:

For all included channels and signals, square each EVM value calculated in step 2, and sum them up.

Divide by the Number of Channels and Signals

Divide the sum of squared EVM values from step

3 by the total number of channels and signals to get the average squared EVM.

Calculate the RMS of EVM

Finally, take the square root of the average squared EVM calculated in step 4 to get the RMS of EVM for all included channels and signals in the OFDM system.

RMS EVM = √(Sum of Squared EVM / Number of Channels and Signals)

The RMS EVM value provides an overall measure of the signal quality across all channels and signals in the OFDM system. Lower RMS EVM values indicate higher signal quality and better accuracy in received signals. Monitoring and optimizing the RMS EVM is crucial in ensuring the reliable performance of OFDM communication systems.

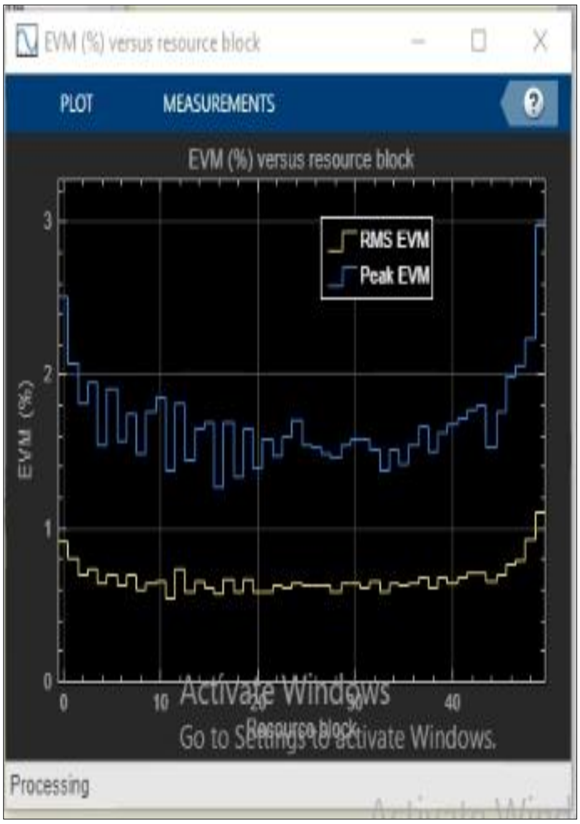

Figure.6 LTE Network resource block

A specific portion of the available radio resources that a mobile network allocates to a user for data transmission or reception. NRB is a fundamental unit used in Long-Term Evolution (LTE)

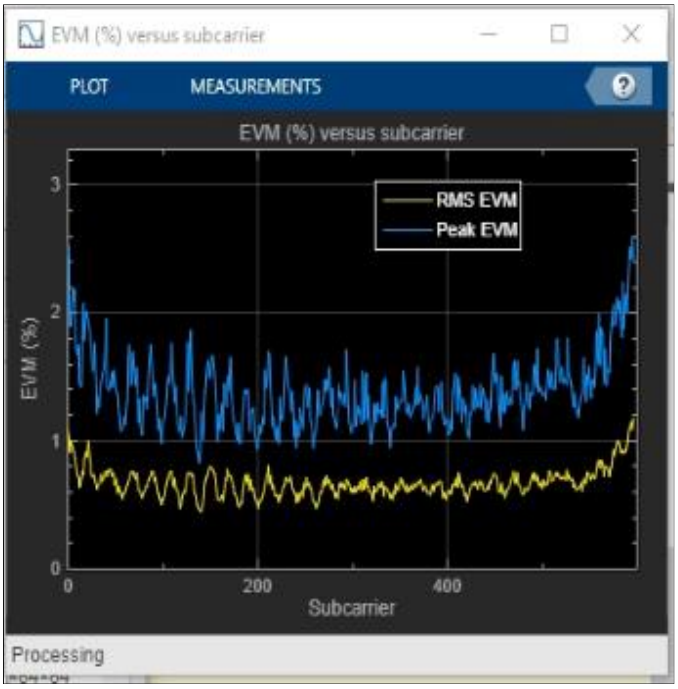

Figure.7 LTE Network subcarrier

The entire LTE bandwidth is divided into a fixed number of subcarriers, and the size of these subcarriers depends on the specific LTE configuration and deployment. Each subcarrier has a fixed frequency spacing, and the total bandwidth is divided equally among the subcarriers.

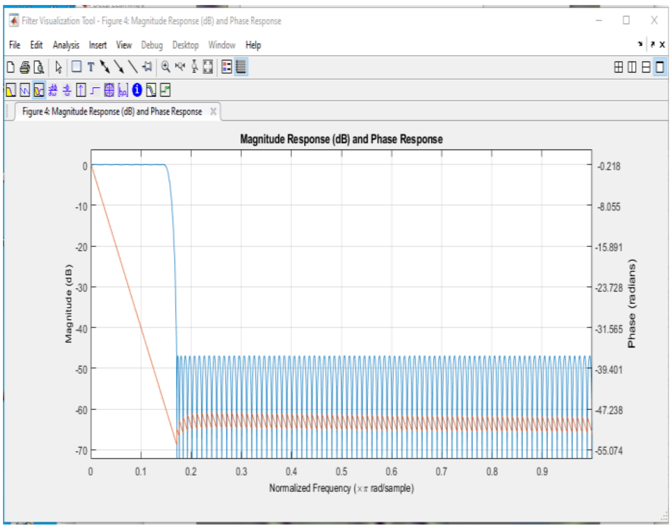

Figure.8 Magnitudes response for all included channels and signals

The frequency domain is divided into subcarriers, as mentioned earlier, which are used to transmit data. Each subcarrier represents a specific frequency bin or channel within the overall system bandwidth. The magnitude response shows the amplitude of each subcarrier's signal.

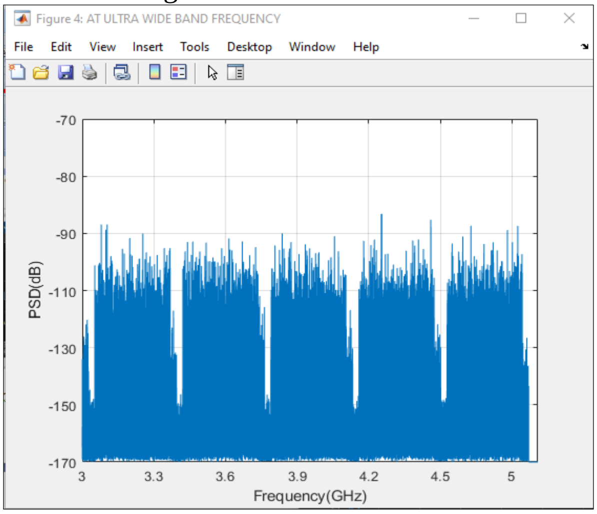

Figure.9 Ultra wide band frequency

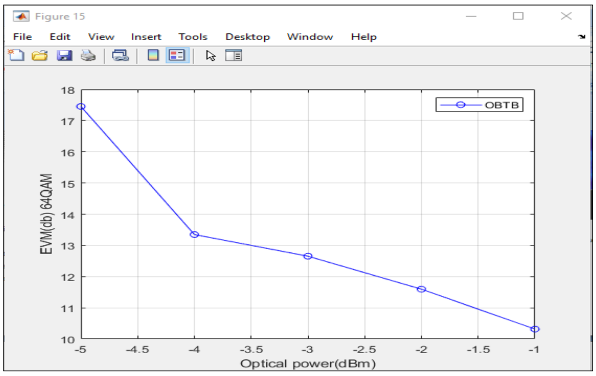

Figure.10 optical power vs.EVM

optical back-to-back (**OBTB**) transmission, Optical power, also known as optical signal power or optical intensity, measures the amount of light energy carried by an optical signal. In an optical communication system

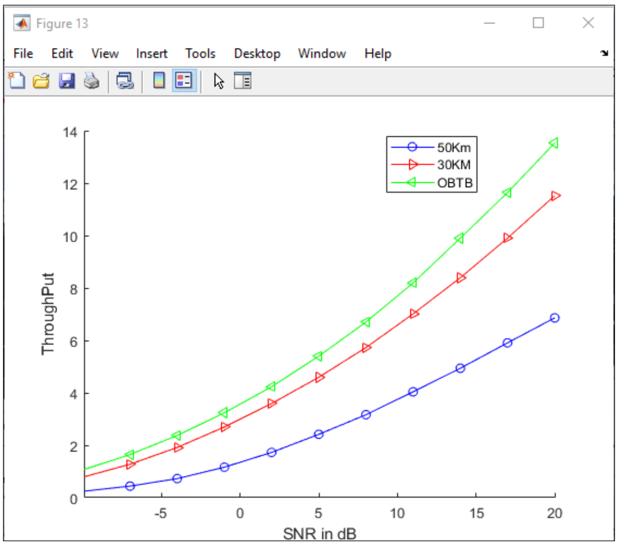

Figure.11 Thought vs. Signal To Noise Ratio

The quality of the communication signal, as measured by the SNR, can influence how well individuals receive, interpret, and understand the thoughts and ideas conveyed through the communication channel.

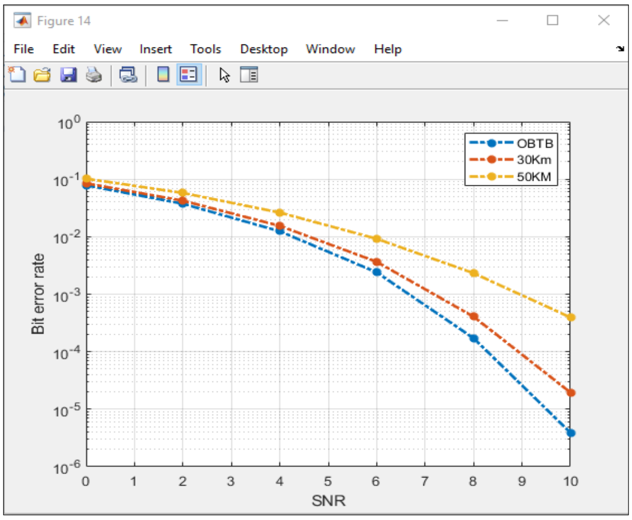

Figure.12 BER Vs.SNR

To illustrate the relationship between BER and SNR for a specific communication system, one can create a BER vs. SNR plot. In this case, we would plot the BER values for the 50 Gbps signal transmitted over the 30 km optical fiber link at various SNR levels. he plot would show how the BER changes as the SNR varies. At higher SNR values, the BER would be lower, indicating better performance, while at lower SNR values, the BER would be higher, indicating degraded performance with more errors

```
ans =

    'The loaded image belongs to the AUTHORIZE'
```

5.5 Authorization Detection

Based on the evaluation of encrypted finger image data transmitted through the LTE network, the system identifies the loaded image as belonging to an authorized user ("The loaded image belongs to the AUTHORIZE"). Additionally, the output indicates that a timing attack has been detected in the carrier dataaggregated code.

6. CONCLUSION

In this proposed security system, we have integrated multiple technologies and techniques to enhance security in an LTE mobile network with the use of ultra-wideband (UWB) carrier aggregation and fingerprint-based input encryption. The system leverages a trained dataset and a classifier to detect attacks and unauthorized access attempts effectively.

In this research approach ,described the various security systems and security systems that are defined standard in LTE networks. The various vulnerabilities of the security system and the security system mobile network. In addition, we reviewed a lot of existing solutions to improve the security of LTE networks. Data on LTE networks is vulnerable to threats and side channel attacks. The proposed solution uses different components to work in sequence. Verification, encryption and decryption, and confidentiality methods are used in this design. Authentication of personal information can prevent unauthorized user access, encryption can protect data transmitted over the network, and private security methods can protect personal. , the simulation presented in the previous output successfully evaluated the Error Vector Magnitudes (EVM) for all included channels and signals in an LTE network. The RMS of the EVM was measured over all symbol-times in the measurement interval, resulting in an overall averaged EVM of 0.664%.

that the received constellation points closely matched the ideal reference points, indicating good signal quality and accuracy in the transmitted data. The cyclic redundancy check (CRC) was performed on the transmitted subframes, and all subframes passed the CRC check, ensuring the integrity of the received data without any errors. the simulation included an additional detection capability, where the system identified the loaded image as belonging to an authorized user, confirming the successful implementation of encrypted finger image data transmission in the LTE network for user authentication..a notable finding was the detection of a timing attack in the carrier dataaggregated code. A timing attack is a potential security vulnerability that needs immediate attention and further investigation to prevent unauthorized access and potential misuse of the system.

References

Bartoletti, S., Giorgetti, A., Conti, A.,2012. UWB sensor radar networks for indoor passive navigation. *In Proceedings of the Tyrrhenian Workshop on Advances in Radar and Remote Sensing (TyWRRS), Naples, Italy, 12–14 September 2012*, pp. 140–145.

Bartoletti, S., Conti, A., Giorgetti, A., Win, M.Z.,2014. Sensor radar networks for indoor tracking. *IEEE Wirel. Commun. Lett. 2014, 3*, pp.157–160.

Bocus, M.J., Piechocki, R.J., 2021. Passive Unsupervised Localization and Tracking using a Multi-Static UWB Radar Network. *In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December* 2021,pp. 1–6.

Bocus, M.J., Chetty, K., Piechocki, R.J., 2021 UWB and WiFi Systems as Passive Opportunistic Activity Sensing Radars. *In Proceedings of the 2021 IEEE Radar Conference (RadarConf21), Atlanta, GA, USA, 7–14 May 2021*, pp. 1–6.

Chang, L.; Chen, X.; Wang, Y.; Fang, D.; Wang, J.; Xing, T.; Tang, Z. FitLoc: Fine-Grained and Low-Cost Device-Free Localization for Multiple Targets Over

Chiani, M., Giorgetti, A., Mazzotti, M., Minutolo, R., Paolini, E., 2009. Target detection metrics and tracking for UWB radar sensor networks. *In Proceedings of the 2009 IEEE International Conference on Ultra-Wideband, Vancouver, BC, Canada, 9–11 September 2009*, pp. 469–474.

Cimdins, M., Schmidt, S.O., Hellbrück, H., 2019. Modeling the Magnitude and Phase of Multipath UWB Signals for the Use in

Passive Localization. *In Proceedings of the 16th Workshop on Positioning, Navigation and Communication, Bremen, Germany, 23–24 October 2019.*

Cimdins, M., Schmidt, S.O., Hellbrück, H., 2020.MAMPI-UWB—Multipath-Assisted Device-Free Localization with Magnitude and Phase Information with UWB Transceivers. *Sensors* 2020, *20*, 7090., [**Google Scholar**] [**CrossRef**]

Cimdins, M., Schmidt, S.O., Hellbrück, H.,2021.Comparison of I/Q- and Magnitude-based UWB Channel Impulse Responses for Device-free Localization. *In Proceedings of the 2021 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 1–3 June 2021;* pp. 1–7. [**Google Scholar**] [**CrossRef**]

Großwindhager, B., Rath, M., Kulmer, J., Bakr, M.S., Boano, C.A., Witrisal, K., Römer, K. SALMA., UWB-based Single-Anchor Localization System using Multipath Assistance. *In Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems, Shenzhen, China, 4–7 November 2018;* pp. 132–144.

Kim, M., Tasaki, T., Yamakawa, S., Millimeter-wave radio tomographic imaging technique using multipath components for indoor localization. *In Proceedings of the 2019 International Symposium on Antennas and Propagation (ISAP), Xi'an, China, 27–30 October 2019;* pp. 1–3.

Kulmer, J., Hinteregger, S., Großwindhager, B., Rath, M., Bakr, M.S., Leitinger, E., Witrisal, K.,2017. Using DecaWave UWB transceivers for high-accuracy multipath-assisted indoor positioning. *In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017.*,pp. 1239–1245. [**Google Scholar**]

Ledergerber, A., D'Andrea, R.,2020. A Multi-Static Radar Network with Ultra-Wideband Radio-Equipped Devices. *Sensors 2020*, *20*, 1599.

Lei, T., Pan, S., Guang, Q.,Wang, K., Yu, Y.,2021. Enhanced Geometric Filtering Method Based Device-Free Localization With UWB Wireless Network. *IEEE Trans. Veh. Technol. 2021*, *70*, 7734–7748.

Li, C., Tanghe, E., Fontaine, J., Martens, L., Romme, J., Singh, G., De Poorter, E., Joseph, W.,2019. Multi-Static UWB Radar-based Passive Human Tracking Using COTS Devices. *arXiv 2021*, arXiv:2109.12856.

Li, C., Tanghe, E., Martens, L., Romme, J., Singh, G., De Poorter, E., Joseph, W.,2022. Device-Free Pedestrian Tracking Using Low-Cost Ultra-Wideband Devices. *IEEE Trans. Instrum. Meas. 2022*, *71*.

Moschevikin, A., Tsvetkov, E., Alekseev, A., Sikora, A.,2016. Investigations on passive channel impulse response of ultra wide band signals for monitoring and safety applications. *In Proceedings of the 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Offenburg, Germany, 26–27 September 2016.* pp. 97–104.

Ninnemann, J., Schwarzbach, P., Jung, A.,Michler, O.,2021. Lab-Based Evaluation of Device-Free Passive Localization Using Multipath Channel Information. *Sensors 2021*, *21*, 2383.

Ninnemann, J., Schwarzbach, P., Michler, O.,2022. Multipath-assisted Radio Sensing and Occupancy Detection for Smart In-house Parking in ITS. *arXiv* 2022, arXiv:2201.06128.

Ninnemann, J., Schwarzbach, P., Schultz, M.,Michler, O.,2022. Multipath-Assisted Radio Sensing and State Detection for the Connected Aircraft Cabin. *Sensors* 2022, *22*, 2859.

Hong, K., Wang, T.,Liu, J., Wang, Y., Shen, Y.,2022. A Learning-Based AoA Estimation Method for Device-Free Localization. *IEEE Commun. Lett.* 2022, *26*, 1264–1267.

Schmidt, S.O., Hellbrück, H.,2021 Detection and Identification of Multipath Interference with Adaption of Transmission Band for UWB Transceiver

Systems. *In Proceedings of the 2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Lloret de Mar, Spain, 29 November–2 December 2021.*, pp. 1–16.

Schmidhammer, M., Siebler, B., Gentner, C. Sand, S., Fiebig, U.C,2022. Bayesian multipath-enhanced device-free localisation: Simulation- and measurement-based evaluation. *IET Microwaves Antennas Propag.* 2022, *16*, 327–337.

Schröder, Y., Wolf, L. InPhase Phase-based Ranging and Localization. *ACM Trans. Sens. Netw. TOSN* 2022, *18*, 1–39.

Sobhani, B., Paolini, E., Giorgetti, A., Mazzotti, M., Chiani, M.,2013. Bayesian tracking in UWB radar sensor networks. In Proceedings of the 2013 *IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, 9–13 June 2013.*, pp. 47–51.

Sobhani, B., Paolini, E., Giorgetti, A.,Mazzotti, M., Chiani, M.,2014. Target Tracking for UWB Multistatic Radar Sensor Networks. *IEEE J. Sel. Top. Signal Process.* 2014, *8*, 125–136.

Tan, J., Zhao, Q., Guo, X., Zhao, X., Wang, G.,2019 Radio tomographic imaging based on low-rank and sparse decomposition. *IEEE Access* 2019, *7*, 50223–50231. [**Google Scholar**] [**CrossRef**]

Tse, D.; Viswanath, P2005. *Fundamentals of Wireless Communication,* Cambridge University Press: Cambridge, UK, 2005.

Wilding, T., Leitinger, E., Muehlmann, U., Witrisal, K.,2020 Modeling human body influence in UWB channels. *In Proceedings of the IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, London, UK, 31 August–3 September 2020.,* pp. 1–6.

Wang, J., Fang, D., Chen, X., Yang, Z.,Xing, T., Cai, L2013. LCS Compressive sensing based device-free localization for multiple targets in sensor networks. *In Proceedings of the 2013 IEEE INFOCOM, Turin, Italy, 14–19 April 2013.*, pp. 145–149.

Zhang, X., Ma, Y., Gong, X., Fu, H. Wang, B., Ning, W., Liang, X.,2022. A training-free multipath enhancement (TFME-RTI) method for Device-Free Multi-target localization. *IEEE Sens. J.* 2022, *22*, 7399–7410.