Received: March 14, 2023. Revised: May 10, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Examining Adversarial Examples Impact on Artificial Intelligence Based Blockage Prediction Systems for Ultra-Wideband Communication in Indoor Environments

Asmaa Ftaimi[1]* **Tomader Mazri**[1]

[1]*Laboratory of Electrical and Telecommunication Engineering Ibn Tofail Science University, Kenitra, Morocco*
* Corresponding author's Email: a.ftaimi@gmail.com

Abstract: Recently, much effort and interest have been devoted to developing accurate and reliable blockage prediction systems. The latest research tends to apply artificial intelligence to enhance blockage prediction systems' accuracy, especially when dealing with non-line-of-sight radio signal propagation. However, AI models can carry inherent vulnerabilities that might damage the relevant system. Therefore, this paper aims to examine the effect of adversarial examples on AI-based blockage prediction systems. By performing adversarial example attacks on the AI-based blockage prediction model, we have shown the drastic impact on root mean square error that has arisen from 0.26 to 0.82 after introducing adversarial examples with 0.08 magnitude. Additionally, we have proposed a defensive approach based on encryption techniques to proactively prevent further compromise of the targeted system. The proposed method not only enhances data privacy but also help to prevent adversarial attacks that exploit transmitted data.

Keywords: Adversarial examples, Blockage prediction, Ultra-wideband, FGSM, Deep neural networks.

1. Introduction

In recent years, the need for full context awareness and perfect knowledge and understanding of the surrounding environment has become an important requirement in several crucial services. Several applications have to turn to the use of a variety of sensors to build efficient positioning systems with high reliability and accuracy. Unlike visual sensing technologies, such as cameras, which can be damaged by rain or lightning [1], Wireless radio communication systems tend to be most suited for this mission as they are hardly influenced by weather conditions. Many wireless radio technologies have been used for object positioning, namely WI-FI (wireless-fidelity), Bluetooth and RFID (radio-frequency-identification). Nevertheless, ultra-wideband (UWB) technology tends to offer better accuracy, a high data throughput, improved temporal resolution, and reduced power usage [2]. UWB represents a radio communication technology that uses short electromagnetic pulses to reliably transmit data. It provides a lot of information with high accuracy, making it the most widely used technology for obstacle detection and context awareness. UWB technologies show great promise for location and positioning systems [3]. They are currently being considered for intelligent transportation systems, robotics, telecommunications, and industrial applications, as shown in Fig. 1.

However, radio signals can be susceptible to several issues, especially attenuation, reflection, and blockage caused by physical obstacles in the indoor environment [4]. Therefore, a key challenge encountered in positioning and context awareness systems lies in designing highly accurate blockage detection and prediction systems. Notably, several experiments have revealed that under non-line-of-sight (NLOS), the received signal might be overwhelmed by the noise resulting from multipath components. Further studies have reported the potential of AI models to substantially improve the accuracy of indoor obstacle identification by significantly improving blockage prediction and recognizing NLOS situations [5].

Indeed, deep learning models have recently been employed in UWB communication to harness the intriguing properties of UWB signals [6]. UWB technology uses electromagnetic waves which propagate over wireless channel carrying high-resolution information about the environment, which considerably contributes to obstacle sensing and identification [7]. Nevertheless, the wireless transmission channel is eligible to be exploited abusively by adversarial attackers who introduce carefully crafted malicious perturbations on the receiver side by using illicit transmitters. This type of attack is particularly relevant for AI-driven blockage prediction systems [8].

Recent studies have clearly indicated that machine learning models carry inherent vulnerabilities that attackers can leverage to perform adversarial attacks on the targeted system [9]. Several adversarial attacks have been recognized by the research community as potentially damaging towards DNN models utilized in wireless communication systems [10]. Some of these adversarial attacks tend to be difficult to detect and are more focused on the signal classification functionality in wireless communication systems, trying to increase the error rates of signal classification. In such attacks, the adversary injects a small, carefully crafted perturbation which alters the original signal and generates a final signal that the receiver would most likely misclassify [11].

The above-mentioned aspects highlight both the feasibility and the simplicity of executing adversarial attacks and creating potentially disruptive impacts on wireless systems. Although, despite the potential threats arising from AI-driven blockage prediction systems, few research studies were dedicated to examining the security aspect of such systems. Additionally, sensing systems are being widely used in highly critical and sensitive applications, although they are vulnerable to adversarial attacks. For instance, UWB communication is commonly employed in mobile and wireless communication services and is being considered in 6G (sixth Generation networks) networks [12].

Therefore, this work seeks to focus on adversarial example attacks that might potentially target AI-driven blockage prediction models in UWB communication systems. This paper will examine extensively the security aspect of these models and their robustness to adversarial examples attacks, its main contribution involves:

- Highlighting the potential threat that adversarial attacks might represent to AI-driven blockage prediction systems.
- Analysing the impact of adversarial attacks on the UWB blockage prediction systems in an indoor environment by designing and performing an FGSM attack and examining its impact on the targeted model.
- Proposing a solution to prevent adversarial examples which mainly enfold encryption techniques that might be considered to protect the integrity of the targeted systems.

In the following section of this paper, we will extensively review the relevant works in the literature and analyse the different approaches adopted regarding the issue of deep learning model security in AI and UWB-based blockage prediction systems.

Afterwards, we will outline the suggested approach to investigate adversarial attacks' impact

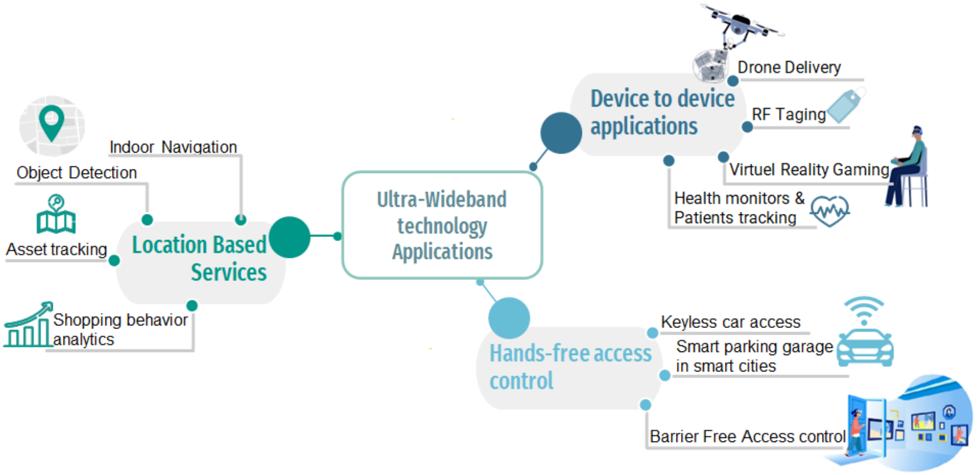

Drone Delivery
Device to device applications
RF Taging
Virtuel Reality Gaming
Health monitors & Patients tracking
Indoor Navigation
Object Detection
Asset tracking
Location Based Services
Ultra-Wideband technology Applications
Shopping behavior analytics
Hands-free access control
Keyless car access
Smart parking garage in smart cities
Barrier Free Access control

Figure. 1 Key application areas of ultra-wideband technology

on such systems. We will present both the theoretical system as well as the experimental setups used in this study. Moreover, the fourth section of this paper is dedicated to presenting the optimisation approach employed to create adversarial perturbations.

The simulation outcomes will be explained in section five where we will highlight the impact of the FGSM attack on our AI-based blockage prediction system. In the sixth section, we will propose a solution that might be effective to protect the targeted systems from adversarial examples.

2. Related works

We will highlight below relevant work focused on security issues emerging from inherent vulnerabilities in AI models.

Despite the significant work regarding the embedding of artificial intelligence in blockage prediction systems [13-18], few research studies have been conducted in the security context [19-20].

Notably, a very limited number of research studies have been devoted to adversarial attacks originating from UWB communication systems [21]. Some research efforts have been devoted to studying jamming attacks that consist of flooding the UWB channel with interfering signals to disrupt legitimate data transmission [22]. Other work has instead focused on eavesdropping on UWB communications that involves capturing sensitive transmitted information [23]. While other research has instead studied spoofing attacks [24], where fraudulent UWB signals are being emitted to fool the receiver into accepting false information.

Fewer papers yet have tackled the issue of security in blockage prediction systems using UWB technologies. Indeed, M. Singh et al. [25] have reviewed the issue of attacks in UWB localization systems, although their work rather concentrates on distance enlargement attacks where the attacker can inject a distorted signal to make it difficult for the receiver to identify the original one.

We believe this research paper will be the first to examine adversarial examples effect on AI-based blockage prediction systems in UWB communication. Moreover, we suggest in this paper a novel approach to defending against these attacks, which differs from the conventional strategies described in the literature.

One of the mitigation techniques that researchers in the area of adversarial learning have proposed to protect the targeted model from adversarial example attacks is adversarial training [26]. This technique consists in introducing adversarial examples into input data to deceive the deep neural network (DNN) model [27]. The existence of several approaches to generate adversarial perturbations renders defensive mechanisms more challenging using this technique. Indeed, the attacker can easily employ a method that hasn't been previously employed by the defender during adversarial training [28]. Additionally, the usage of several techniques to generate adversarial examples during adversarial training might significantly reduce the target model's accuracy [29].

Another defensive mechanism, known as defensive distillation [30], has been proposed by N. Papernot et al. [31] to reduce the drastic effect of adversarial examples on DNN models. This approach relies on the distillation method suggested by Hinton et al. [32] to achieve a reduced DNN architecture and therefore optimize computing resources without degrading the model's accuracy. The main idea underlying this technique consists in extracting the class probability vector generated using an initial DNN architecture to proceed to the training of a second DNN with diminished dimensionality. It has been shown that this technique can reduce the robustness of adversarial examples from 95% to less than 0.5% while having a low impact on the architecture and the model accuracy [33]. However, this defensive mechanism remains not a universal approach [29], in the sense that it cannot be fully generalized to all types of attacks and different AI-driven systems.

Our proposed solution is mainly driven by the data privacy approach, it relies on applying encryption algorithms to prevent the attacker from accessing the data used by the AI model and therefore, render the task of generating robust adversarial examples practically unachievable. Furthermore, our method is highly adaptable as it can be applied regardless of the strategy employed by the opponent to craft the adversarial perturbations introduced to target the DNN model. Moreover, it can be generalized as a defensive strategy against data poisoning and evasion attacks that consist in introducing carefully crafted perturbations to induce AI models into generating inaccurate results, since it applies an encryption algorithm on data before its transmitted to the AI model, which ensures that attackers cannot intercept and access the transmitted data.

3. System model and experimental setup

Adversaries may adopt different attack strategies according to their targets, their capabilities, and their knowledge of their attack's target system. But

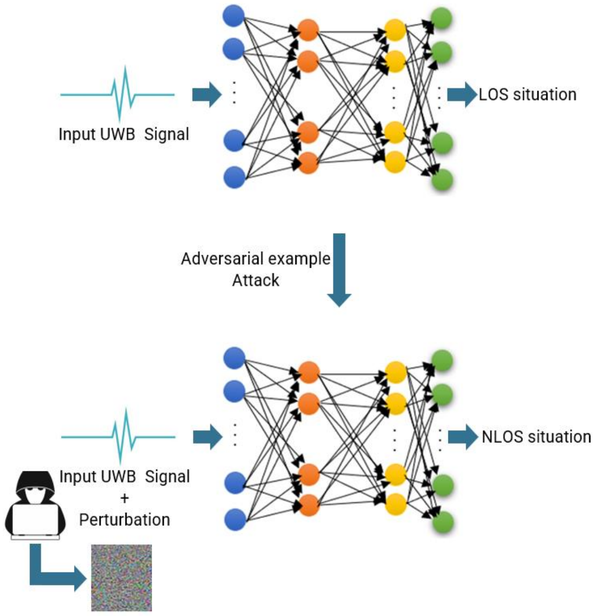


Figure. 2 FGSM attack process carried out on AI-based blockage prediction system in UWB communication

generally, executing an adversarial attack consists purely of resolving a challenging optimization problem [34]. Indeed, most often, the attacker aims to identify an imperceptible perturbation ɳ to append the input data x of the DNN model to generate completely different output from the one expected if no adversarial example is involved as illustrated in Fig. 2. Moreover, the most effective approach to identifying such a perturbation consists of maximizing the cost function, which serves to determine the disparity within the model's forecasted values and the expected output as illustrated in (1) and (2):

$$x' = x + \eta \quad (1)$$

Where $\eta = argmin \{\mu \, \epsilon \, \mathbb{R} : F\theta(x) \neq F\theta(x + \mu)\}$

$$\mathcal{L}(\theta_i, x_i) = y_i - F\theta(x_i), \theta_i \, \epsilon \, \theta, x_i \, \epsilon X, y_i \, \epsilon Y \quad (2)$$

Where $\theta = \{\theta_1, \theta_2, \dots, \theta_n\}$, $X = \{x_1, x_2, \dots, x_n\}$ and $Y = \{y_1, y_2, \dots, y_n\}$ are respectively the DNN model's parameters, the input data and the output data vectors with n elements, while F is a representative function of the DNN model that minimizes the cost function.

In this work, we will consider a communications setup where an AI-based blockage prediction system uses data collected from UWB antennas placed in an indoor environment. The blockage prediction system provides a real-time perception of the ambient environment and identifies existing obstacles in the surrounding area through the recognition of non-line of sight (NLOS) situations [35] as shown in Fig. 3.

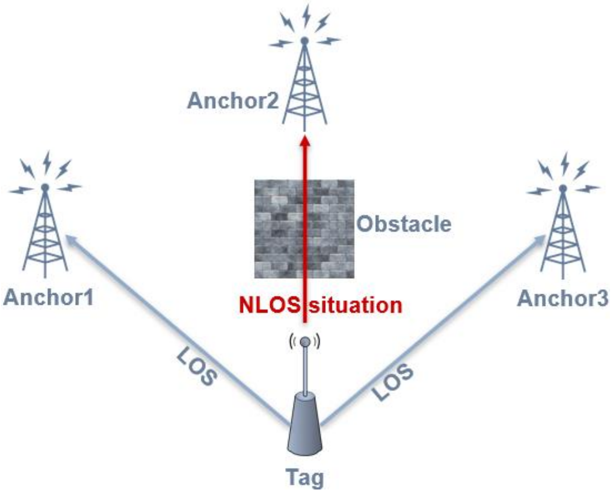


Figure. 3 Scenario of a direct path between the tag and the anchors (LOS) and blockage situation (NLOS) due to the existence of an obstacle between the tag and the anchor2

We designed our deep learning model, to thoroughly address this challenge of recognizing blocking situations arising from encountered obstacles. Once the deep learning model is well-trained, it can be used to determine if the UWB tag is experiencing an NLOS situation.

To simplify our setup, we will only consider a single anchor that will communicate with the UWB tag. The tag will be attached to the tracked mobile object while the Anchor is used to capture the UWB signal emitted by the Tag. Nevertheless, to determine the NLOS situations we will equip our UWB system with a Deep Learning model that will serve to recognize the blockage situations caused by the presence of obstacles [17].

The Deep learning model used in this simulation is composed of 6 layers as illustrated in Fig. 4. To achieve maximum accuracy, we have performed hyperparameters tuning to determine both the layers and the neurons that would be used in the DNN model. We have also opted for RELU and SOFTMAX as activation functions to transform the data representation as it flows through the DNN models' layers. The sigmoid function has been rather applied in the last layer to assign the appropriate classification to each input data. Indeed, this study focuses on a binary classification problem. Hence, class "1" is assigned to the NLOS situations while "0" represents the class associated with the LOS situations.

The dataset used in this setup is developed by K. Bregar et al. [8] and has been generated using an SNPN-UWB board within a DecaWave DWM1000 UWB radio module. All the observations have been

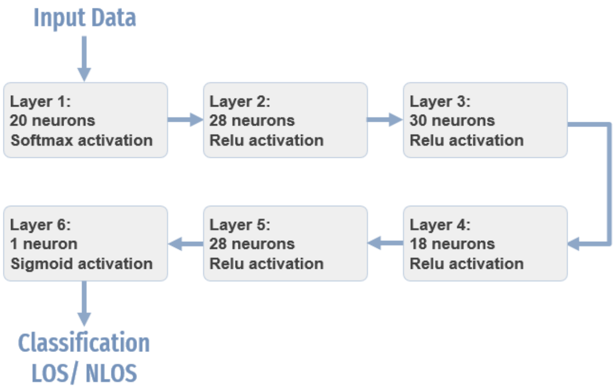


Figure. 4 The deep learning model architecture employed for LOS/NLOS classification problem

performed at seven different indoor locations (two different offices, a small apartment, a workshop, a common room equipped with both kitchen and a small living room, a sleeping room, and a boiler-room) [1] [36]. From each indoor location, 3000 data samples for LOS situations and 3000 data samples for NLOS situations have been collected.

Overall, 42,000 samples have been obtained that included 21,000 data samples for LOS channel conditions and 21,000 data samples for NLOS conditions distributed.

4. Adversarial examples attack

Our research addresses the issue of security of AI-driven intelligent environment perception systems. Therefore, we will review an adversarial attack scenario where the attacker intends to remotely corrupt our intelligent blockage prediction system by compromising the integrity of the deep learning model input data and hence leading to serious performance degradation within our intelligent obstacle sensing system. Effectively, the attacker may introduce perturbations into our input data that depict the signal obtained from the UWB tag. These perturbations have been carefully crafted to be imperceptible while misleading the model to produce incorrect classifications.

In this study we have employed fast-gradient-sign method known as FGSM attack. The latter has been utilized in the building process of perturbations specifically tailored to target our AI-based blockage prediction system.

This intuitive attack developed by Goodfellow et. al. [19] has been conceived to attack DNN models by employing gradients. The premise behind this attack relies on the tuning of the input data to maximize the loss function based on the gradients used in the backpropagations as follows in (3):

$$x^* = x + \varepsilon sign(\Delta_x \mathcal{L}_\theta(x; y)) \quad (3)$$

Where $\mathcal{L}_\theta$ represent the utilized loss function at the DNN model's training and θ represents the DNN model's parameters. The $sign()$ indicates the sign function and ε indicates the perturbation magnitude.

In our simulation, we have considered a data split of 80:20, therefore 33600 data samples were used for the model training while 8400 data samples were exploited in the validation phase. We have carried out a pre-processing of our data. In this stage, we have performed feature engineering, which consists in retrieving features from raw data to identify the best representation for the data samples that approaches the task being addressed by the DNN model.

During the feature selection step, we have implemented the Univariate Selection methods that involve applying statistical measures such as the correlation between the input and output variables calculated using Chi-Squared to determine the features to be selected [37]. The choice of this technique was driven by its reduced computational time and lower memory requirements when compared to other feature selection methods. Thus, we have identified the features to be used following the percentile that provides the highest score. Once this process was accomplished, we retained 4% of the features from raw data, i.e., 41 selected features. Given that our intelligent blockage prediction system deals with a binary classification problem (LOS or NLOS situation), the most suitable loss function to apply in our case would be binary cross entropy. To obtain the best accuracy, we have used a batch sized 450 and we have set up epochs at 600.

5. Simulation results

The obtained result after embedding DNN model are extensively described in the third section. Indeed, using the previous hyperparameters, we achieve a test accuracy of 0.91 while the obtained test loss is 0.207 as mentioned in Figs. 5 and 6. We have also evaluated the reliability of our deep learning model by applying the root mean square error method and we have found a RMSE of 0.26.

Our approach consists primarily of exploring the scenario where the opponent possesses a full knowledge of the targeted DNN model. Such attack is commonly defined as "white-box" attack. The FGSM attack suggested by Goodfellow et al [19] is performed by introducing carefully crafted small perturbations that maximize the loss function mainly used to train the model to achieve maximum accuracy.

To assess the accuracy of the predicted values produced by the DNN model, we have applied error

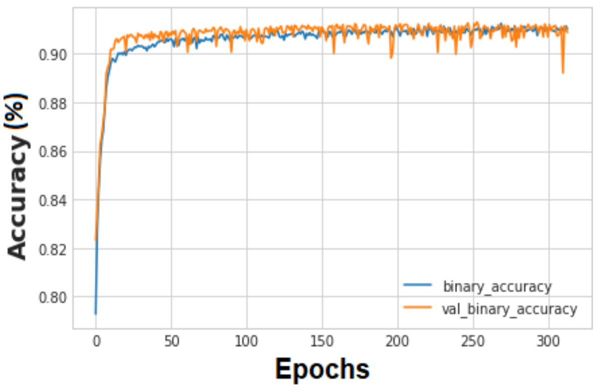


Figure. 5 DNN model’s accuracy at the training and the validation steps where the blue line illustrates the training accuracy while the orange one corresponds to the validation accuracy

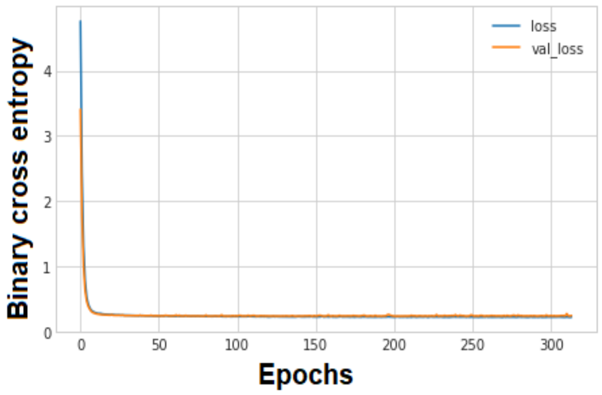


Figure. 6 Graph of the training and the validation loss where the blue line characterises the training loss while the orange one corresponds to the validation loss

Table 1. RMSE measured for a range of perturbation magnitude after carrying out FGSM attack

Perturbation Magnitude (Epsilon)	RMSE
0.01	0.42
0.02	0.58
0.03	0.68
0.04	0.75
0.05	0.78
0.06	0.80
0.07	0.81
0.08	0.82
0.09	0.82
0.1	0.82

functions.

We have implemented the root mean square error (RMSE) method [38] to carry out an estimation of average disparity of predicted values from their corresponding observations. The computed outcomes are reported in Table 1.

6. Proposed solution

Data privacy can be an important approach to consider in preventing adversarial attacks. Data privacy might be effective to prevent adversarial examples by restricting amount of information that an attacker could access to potentially craft malicious perturbations capable of deceiving the model. Our proposed approach involves performing backhaul data encryption before its transmitted from the anchors to the final AI model. In this way, encryption can help to ensure that the data used by AI model remains private, even when multiple anchors are involved in the blockage prediction system.

Our method consists of encrypting data using asymmetric algorithms using a public key before being transmitted to the server where the AI model is executed. The received data is thereafter decrypted by the server using the private key. Afterwards, decrypted data is processed by AI model to predict the classification of the blockage situation: either LOS or NLOS situation as illustrated in Fig. 7.

To comprehensively assess the proposed approach, we need to examine in detail the impact of encryption on the performance of the blockage prediction system. While encryption can be an efficient approach to protecting data in AI-based blockage prediction systems, it can also introduce additional challenges that must be diligently addressed. Indeed, encryption algorithms can be computationally expensive, which may potentially

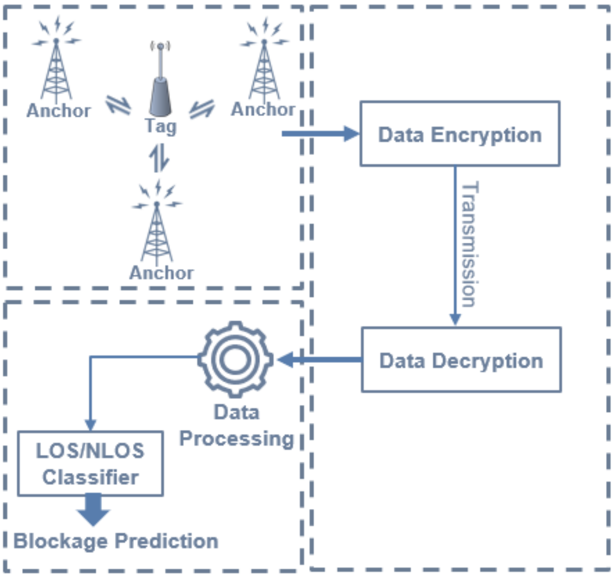
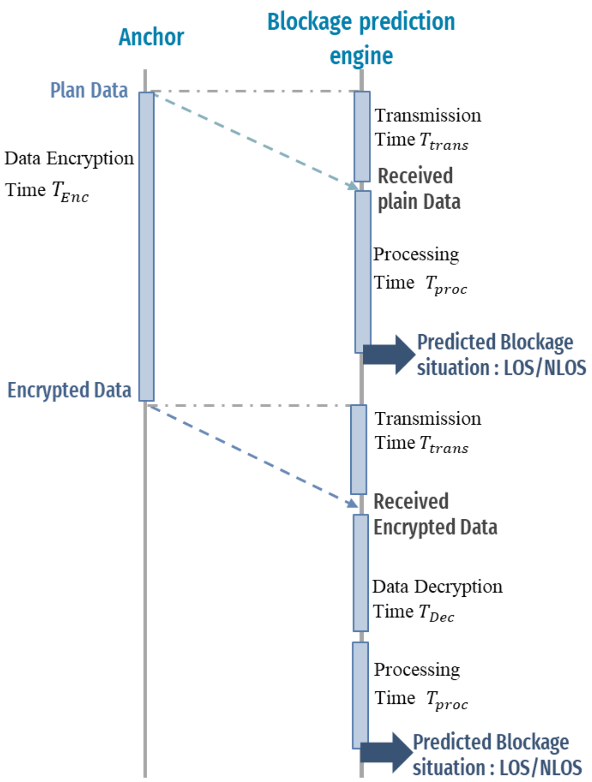


Figure. 7 Blockage prediction process using encryption techniques or UWB communication systems



Anchor
Blockage prediction engine
Plan Data
Data Encryption Time T_{Enc}
Transmission Time T_{trans}
Received plain Data
Processing Time T_{proc}
Predicted Blockage situation : LOS/NLOS
Encrypted Data
Transmission Time T_{trans}
Received Encrypted Data
Data Decryption Time T_{Dec}
Processing Time T_{proc}
Predicted Blockage situation : LOS/NLOS

Figure. 8 Blockage prediction process for both scenarios using encryption and without encryption

slow down the processing time of the model.

Therefore, we will explore a setup using TDoA (time difference of arrival) algorithm. The blockage prediction process is initiated from the tag throughout a flash signal emitted to all anchors. Each anchor transmits encrypted backhaul data to the blockage prediction Engine. The latter decrypts the received encrypted data then processes it and computes the LOS situation and finally responds to the anchor with the predicted blockage situation.

Fig. 8. Illustrates the process of blockage prediction considering both scenarios: with and without encryption.

The estimated time normally taken by the blockage prediction engine to reply to the blink signal when plain data is transmitted from the anchor to the AI model is determined by the Eq. (4):

$$T_{reply} = T_{trans} + T_{proc} \tag{4}$$

Where T_{reply}, T_{trans} and T_{proc} are respectively the time to reply, the time spent in data transmission and the time required for data processing to predict the Los situation.

As explained above, the proposed process requires the encryption of data using the asymmetric key before it is transmitted to the server. In this case, the expected time period needed by the blocking prediction model to respond to the blink signal is assessed by Eq. (5):

$$T_{reply} = T_{trans} + T_{Enc} + T_{Dec} + T_{proc} \tag{5}$$

Where T_{reply}, T_{trans}, T_{Enc}, T_{Dec}, and T_{proc} are respectively the time to reply, the time spent in data transmission, the delay due to data encryption using the public key, the delay needed for data decryption using the private key and the time required for data processing to predict the Los situation.

Therefore, data encryption will add a delay to the computation time consumed by the blockage prediction system estimated by $T_{Enc} + T_{Dec}$. As a result, it is crucial to select the appropriate encryption algorithm which not only guarantees a high level of data privacy but also reduces encryption and decryption delays.

In this way, our method leads to the optimization problem defined in Eq. (6). That consists in determining the algorithm that minimizes the time delay obtained in the previous paragraph.

$$\mathcal{L}_{min} = \underset{\mathcal{L} \in \mathcal{D}}{\operatorname{argmin}}(T_{Enc} + T_{Dec}) \tag{6}$$

Where $\mathcal{L}_{min}$, $\mathcal{L}$, $\mathcal{D}$, T_{Enc} and T_{Dec} are respectively the optimal algorithm, encryption algorithm, the distribution of encryption algorithms, the delay due to data encryption using the public key, the delay needed for data decryption using the private key.

7. Discussion

This work has addressed the security issue of AI-based blockage prediction systems for UWB communication in indoor environments. The approach we have considered is designed to cover several aspects, notably the study of the impact of adversarial attacks on AI-driven blockage prediction systems and the proposition of a defensive strategy to reduce adversarial examples' robustness.

Indeed, we have designed a deep learning model to efficiently predict non-line-of-sight situations. Later, we performed the FGSM attack to generate carefully crafted malicious perturbations. With the hypothesis of white-box attack [39] that holds significant importance since as long as the adversary has a comprehensive understanding of the targeted system, he can effectively build quasi-imperceptible perturbations [40]. Furthermore, we have shown that even attacks with small noise magnitudes have significantly impacted the predictions of the targeted model with a large error rate. For example, we noticed a rise of RMSE up to 0,42 for a noise magnitude of epsilon 0.001. With higher perturbation magnitudes, the error rate exponentially increased making the model unable to produce correct classifications. According to the result obtained in the previous simulation, the RMSE has reached 0,8 with an epsilon of 0,06.

Furthermore, we have considered data privacy as a key element in our defensive strategy to protect the AI model from adversarial examples. We have proposed a method based on data encryption to protect it from unauthorized access. Indeed, encryption techniques help to prevent attackers from manipulating input data without being detected. Hence, the proposed method is designed to meet the privacy, integrity and availability requirements of the blockage prediction system [41].

However, as mentioned in the section above, encryption can generate delays that might slow down the processing time of the AI model and thus impact its performance. This observation has been taken into consideration when selecting the encryption algorithm that would minimise the delays resulting from data encryption and decryption.

In this paper, we have developed the conceptual and theoretical basis by defining the optimization problem which is the main key in our proposed method. We are on the way to validating these results by simulation in our future work. We intend to run an extensive comparative study of encryption algorithms to select the most suitable to our experimental setup and asses both the security and the performance impact after the implementation of encryption algorithms in the AI-based blockage prediction system.

8. Conclusion

The study conducted in this paper has demonstrated the potential threat posed by adversarial examples against deep neural networks employed in blockage prediction systems. In this work, we have suggested a comprehensive study in which we have highlighted the drastic effect of adversarial attacks on DNN models employed to predict NLOS situations for UWB communication systems. Throughout the study conducted in paper, we have established the theoretical basis of our proposed method and have extensively explained the importance of addressing this trade-off between model robustness to adversarial attacks and the subsequent impact on AI model performance in future research projects to enable secure and reliable use of AI technology, promoting its many advantages while mitigating its risks.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, A. FTAIMI and T. MAZRI; methodology, A. FTAIMI; software, A. FTAIMI; validation, A. FTAIMI and T. MAZRI; formal analysis, A. FTAIMI; investigation, A. FTAIMI; resources, A. FTAIMI; data curation, A. FTAIMI; writing—original draft preparation, A. FTAIMI; writing—review and editing, A. FTAIMI; visualization, A. FTAIMI; supervision, T. MAZRI; project administration, A. FTAIMI and T. MAZRI; funding acquisition, A. FTAIMI.

References

[1] Guesmi and I. Alouani, “Adversarial Attack on Radar-based Environment Perception Systems”, 2022, doi: 10.48550/ARXIV.2211.01112.

[2] Y. Gao, O. Postolache, Y. Yang, and B. Yang, “UWB System and Algorithms for Indoor Positioning”, In: *Proc. of 2021 Telecoms Conference (ConfTELE)*, Leiria, Portugal, pp. 1–6, 2021, doi: 0.1109/ConfTELE50222.2021.9435577.

[3] J. Wu, Z. Zhang, S. Zhang, Z. Kuang, and L. Zhang, “UWB Positioning Algorithm Based on Fuzzy Inference and Adaptive Anti-NLOS Kalman Filtering”, *Applied Sciences*, Vol. 12, No. 12, p. 6183, 2022, doi: 10.3390/app12126183.

[4] O. Onalaja, M. Adjrad, and M. Ghavami, “Ultra-wideband-based multilateration technique for indoor localisation”, *IET Communications*, Vol. 8, No. 10, pp. 1800–1809, 2014, doi: 10.1049/iet-com.2013.0815.

[5] H. Wymeersch, S. Marano, W. M. Gifford, and M. Z. Win, “A Machine Learning Approach to Ranging Error Mitigation for UWB Localization”, *IEEE Trans. Commun.*, Vol. 60, No. 6, pp. 1719–1728, 2012, doi: 10.1109/TCOMM.2012.042712.110035.

[6] X. Ye and Y. Zhang, “Research on UWB positioning method based on deep learning”, In: *Proc. of 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, Harbin, China, pp. 1505–1508, 2020, doi: 10.1109/ICMCCE51767.2020.00330.

[7] R. Cicchetti, E. Miozzi, and O. Testa, “Wideband and UWB Antennas for Wireless Applications: A Comprehensive Review”, *International Journal of Antennas and*

Propagation, Vol. 2017, pp. 1–45, 2017, doi: 10.1155/2017/2390808.

[8] K. Bregar and M. Mohorcic, "Improving Indoor Localization Using Convolutional Neural Networks on Computationally Restricted Devices", *IEEE Access*, Vol. 6, pp. 17429–17441, 2018, doi: 10.1109/ACCESS.2018.2817800.

[9] M. Sadeghi and E. G. Larsson, "Adversarial Attacks on Deep-Learning Based Radio Signal Classification", *IEEE Wireless Commun. Lett.*, Vol. 8, No. 1, pp. 213–216, Feb. 2019, doi: 10.1109/LWC.2018.2867459.

[10] Y. E. Sagduyu, T. Erpek, and Y. Shi, "Adversarial Machine Learning for 5G Communications Security", *Game Theory and Machine Learning for Cyber Security*, 1st ed., C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, Eds. Wiley, 2021, pp. 270–288. doi: 10.1002/9781119723950.ch14.

[11] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial Examples in the Physical World", *in Artificial Intelligence Safety and Security*, 1st ed., R. V. Yampolskiy, Ed. First edition. | Boca Raton, FL : CRC Press/Taylor & Francis Group, 2018.: Chapman and Hall/CRC, 2018, pp. 99–112. doi: 10.1201/9781351251389-8.

[12] Z. R. M. Hajiyat, A. Ismail, A. Sali, and M. N. Hamidon, "Antenna in 6G wireless communication system: Specifications, challenges, and research directions", *Optik*, Vol. 231, p. 166415, Apr. 2021, doi: 10.1016/j.ijleo.2021.166415.

[13] J. Yan, L. Zhao, J. Tang, Y. Chen, R. Chen, and L. Chen, "Hybrid Kernel Based Machine Learning Using Received Signal Strength Measurements for Indoor Localization", *IEEE Trans. Veh. Technol.*, Vol. 67, No. 3, pp. 2824–2829, Mar. 2018, doi: 10.1109/TVT.2017.2774103.

[14] L. Nosrati, M. S. Fazel, and M. Ghavami, "Improving Indoor Localization Using Mobile UWB Sensor and Deep Neural Networks", *IEEE Access*, Vol. 10, pp. 20420–20431, 2022, doi: 10.1109/ACCESS.2022.3151436.

[15] L. Zhang, Y. Li, Y. Gu, and W. Yang, "An efficient machine learning approach for indoor localization", *China Commun.*, Vol. 14, No. 11, pp. 141–150, Nov. 2017, doi: 10.1109/CC.2017.8233657.

[16] C. H. Hsieh, J. Y. Chen, and B. H. Nien, "Deep Learning-Based Indoor Localization Using Received Signal Strength and Channel State Information", *IEEE Access*, Vol. 7, pp. 33256–33267, 2019, doi: 10.1109/ACCESS.2019.2903487.

[17] S. Marano, W. Gifford, H. Wymeersch, and M. Win, "NLOS identification and mitigation for localization based on UWB experimental data", *IEEE J. Select. Areas Commun.*, Vol. 28, No. 7, pp. 1026–1035, Sep. 2010, doi: 10.1109/JSAC.2010.100907.

[18] K. Gururaj, A. K. Rajendra, Y. Song, C. L. Law, and G. Cai, "Real-time identification of NLOS range measurements for enhanced UWB localization", In: *Proc. of 2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Sapporo, pp. 1–7, 2017, doi: 10.1109/IPIN.2017.8115877.

[19] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples", *CoRR*, Vol. abs/1412.6572, 2014, doi: 10.48550/ARXIV.1412.6572.

[20] A. Athalye, N. Carlini, and D. Wagner, "Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples", In: *Proc. of International Conference on Machine Learning*, 2018, doi: 10.48550/ARXIV.1802.00420.

[21] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Over-the-Air Adversarial Attacks on Deep Learning Based Modulation Classifier over Wireless Channels", In: *Proc. of 54th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, 2020, doi: 10.48550/ARXIV.2002.02400.

[22] P. Mykytyn, M. Brzozowski, Z. Dyka, and P. Langendoerfer, "Jamming Detection for IR-UWB Ranging Technology in Autonomous UAV Swarms", In: *Proc. of 2021 10th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro, pp. 1–6, 2021, doi: 10.1109/MECO52532.2021.9460250.

[23] C. Herold, T. Doeker, J. M. Eckhardt, and T. Kurner, "Investigation of Eavesdropping Opportunities in a Meeting Room Scenario for THz Communications", In: *Proc. of 2022 16th European Conference on Antennas and Propagation (EuCAP)*, Madrid, Spain, pp. 1–5, 2022, doi: 10.23919/EuCAP53622.2022.9769432.

[24] Z. E. Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications", *Vehicular Communications*, Vol. 23, p. 100214, 2020, doi: 10.1016/j.vehcom.2019.100214.

[25] M. Singh, P. Leu, A. M. Abdou, and S. Capkun, "UWB-ED: Distance Enlargement Attack

Detection in Ultra-Wideband", *IACR Cryptol. ePrint Arch.*, Vol. 2019, p. 1349, 2019, doi: 10.3929/ETHZ-B-000309346.

[26] W. Zhao, S. Alwidian, and Q. H. Mahmoud, "Adversarial Training Methods for Deep Learning: A Systematic Review", *Algorithms*, Vol. 15, No. 8, p. 283, 2022, doi: 10.3390/a15080283.

[27] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, "Ensemble Adversarial Training: Attacks and Defenses", *ArXiv*, Vol. abs/1705.07204, 2017, doi: 10.48550/ARXIV.1705.07204.

[28] S. Park and J. So, "On the Effectiveness of Adversarial Training in Defending against Adversarial Example Attacks for Image Classification", *Applied Sciences*, Vol. 10, No. 22, p. 8079, 2020, doi: 10.3390/app10228079.

[29] A. Shafahi, M. Najibi, Z. Xu, J. Dickerson, L. S. Davis, and T. Goldstein, "Universal Adversarial Training", *AAAI*, Vol. 34, No. 04, pp. 5636–5643, 2020, doi: 10.1609/aaai.v34i04.6017.

[30] F. O. Catak, M. Kuzlu, E. Catak, U. Cali, and O. Guler, "Defensive Distillation-Based Adversarial Attack Mitigation Method for Channel Estimation Using Deep Learning Models in Next-Generation Wireless Networks", *IEEE Access*, Vol. 10, pp. 98191–98203, 2022, doi: 10.1109/ACCESS.2022.3206385.

[31] N. Papernot and P. McDaniel, "On the Effectiveness of Defensive Distillation", *ArXiv*, Vol. abs/1607.05113, 2016, doi: 10.48550/ARXIV.1607.05113.

[32] G. Hinton, O. Vinyals, and J. Dean, "Distilling the Knowledge in a Neural Network", *ArXiv*, Vol. abs/1503.02531, 2015, doi: 10.48550/ARXIV.1503.02531.

[33] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks", In: *Proc. of 2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, pp. 582–597, 2016, doi: 10.1109/SP.2016.41.

[34] N. Papernot, P. M. Daniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical Black-Box Attacks against Machine Learning", In: *Proc of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates, pp. 506–519, 2017, doi: 10.1145/3052973.3053009.

[35] K. Bregar, A. Hrovat, M. Mohorcic, and T. Javornik, "Self-Calibrated UWB based device-free indoor localization and activity detection approach", In: *Proc. of 2020 European Conference on Networks and Communications (EuCNC)*, Dubrovnik, Croatia, pp. 176–181, 2020, doi: 10.1109/EuCNC48522.2020.9200968.

[36] H. Xu, Y. Ma, H. C. Liu, D. Deb, H. Liu, J. L. Tang, and A. K. Jain, "Adversarial Attacks and Defenses in Images, Graphs and Text: A Review", *International Journal of Automation and Computing*, Vol. 17, No. 2, pp. 151–178, 2020, doi:10.1007/s11633-019-1211-x.

[37] A. Poulose and D. S. Han, "Feature-Based Deep LSTM Network for Indoor Localization Using UWB Measurements", In: *Proc. of 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Jeju Island, Korea (South), pp. 298–301, 2021, doi: 10.1109/ICAIIC51459.2021.9415277.

[38] W. Wang and Y. Lu, "Analysis of the Mean Absolute Error (MAE) and the Root Mean Square Error (RMSE) in Assessing Rounding Model", *IOP Conf. Ser.: Mater. Sci. Eng.*, Vol. 324, p. 012049, 2018, doi: 10.1088/1757-899X/324/1/012049.

[39] J. Ebrahimi, A. Rao, D. Lowd, and D. Dou, "HotFlip: White-Box Adversarial Examples for Text Classification", In: *Proc of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*, Melbourne, Australia, pp. 31–36, 2018, doi: 10.18653/v1/P18-2006.

[40] N. Carlini and D. Wagner, "Towards Evaluating the Robustness of Neural Networks", In: *Proc. of 2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp. 39–57, 2017, doi: 10.1109/SP.2017.49.

[41] A. Shafahi, W. R. Huang, C. Studer, S. Feizi, and T. Goldstein, "Are Adversarial Examples Inevitable?", *ArXiv*, Vol. abs/1809.02104, 2018, doi: 10.3929/ETHZ-B-000460350.