Modelling and Analysis of Relay Attack Devices for Passive-Entry-Passive-Start Wireless Systems

Sowjanya Rath [1], Dr. Altaf Q H Badar [2], V Kiran Bharadwaj [3]

[1]Department Of Electrical Engineering, National Institute of Technology, Warangal, Telangana, India
[2]Department Of Electrical Engineering, National Institute of Technology, Warangal, Telangana, India
[3]Department Of Electronics & Communication Engineering, National Institute of Technology Durgapur, West Bengal, India
sree21336@student.nitw.ac.in

Abstract: Passive-entry-passive-start (PEPS) is a wireless communication system that enables a driver to enter and start their vehicle without the need of a physical key. In PEPS system, the vehicle sends low-power LF signal to communicate with the key-fob. If the key is in the vicinity of the automobile, it sends a RF signal which the vehicle senses and unlocks the door. In this work, we show how vulnerable these systems can be to external attacks using relay devices. In a relay attack, the objective is to amplify the vehicle signal to transmit to longer distances such that it can communicate with the key-fob and unlock the door, without the knowledge of the owner. This work includes a model of the relay devices developed using MATLAB, as well as a detailed explanation of an attack scenario. A distance-based test case has also been included to conclude the attack. In the introduction section, a few popular techniques which can be used to mitigate relay attacks have been reviewed.

Keywords: relay attack, Passive Entry passive start (PEPS), power budget analysis, Radio frequency (RF), Low Frequency (LF), Low Noise Amplifier (LNA)

1. Introduction

As modern vehicles continue to be more reliant on technology, most research being done in the automotive industry is on the electronics and software part rather than the mechanical engineering. These vehicles host multiple Electronic Control Units (ECUs), interconnected to each other through internal networks to various sensors. This, however, has introduced the threat of cyber-attacks, which can have a devastating impact on the reliability of these vehicles [1].

One such feature introduced to enhance the convenience of the user is the Smart Key System. The first form of smart key systems involved remote access to the vehicle where the users were able to open their car remotely by pressing a button on their key fobs. Passive-entry-passive-start (PEPS) is a newer technology that allows customers to get into their cars and get them started while keeping their car keys in their wallets. [2]. It works based on RF Identification (RFID). If the user triggers the door handle, a low frequency signal is sent from the vehicle to the key-fob. The key-fob responds to the LF signal by reverting to the vehicle an RF signal. If the vehicle decodes the received RF signal, it will automatically unlock the door for the user [3].

Since the vehicles send a very low-power signal, the ability to interact with the fob indicates the proximity of the user. This introduces the threat of relay attacks. A relay attack uses simple amplifier blocks which can transmit the signal over longer distances. Even adding a layer of encryption fails to protect the system as the relay just needs to boost the signal rather than decode it.

Relay attacks can be broadly classified into two types: (i) LF and (ii) RF attacks. An LF signal is sent from the car to the fob through the LF attack (as in Fig 1). RF relay attack relays both an LF signal from the car as well as an RF signal from the fob to the car. As an RF signal is also transmitted, the possible attack distance for an RF relay attack is greater (up to 1 km) [3].

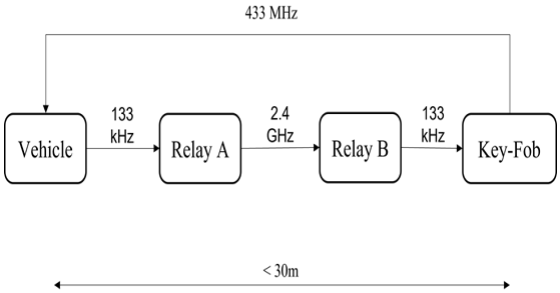

***Fig 1**: LF relay attack block diagram*

The work proposed here models the relay attack extensively on MATLAB and Simulink along with results on a component level after each stage. Modelling of an LF relay attack and development of the front-end architecture of the two blocks, i.e. both relays is done. One near the vehicle and the other being closer to the key fob This work aims to provide a comprehensive understanding of the attack and show the vulnerabilities of the smart key. A Power Budget Analyzer is used up in this paper. It is to make sure a system or device functions within its power limits, and the total power consumption of the system or its components is calculated. The software then calculates and shows the system's expected power consumption based on the user's consumption levels.

https://doi.org/10.1049/icp.2023.1530

2. Literature Survey

In order to avoid relay attacks, certain methods have been proposed in [2] and [3] to counteract the attack. These include trivial methods like using a Faraday box to block the signals or taking out the battery from the key-fob when not in use [2]. Another technique proposed was to implement a secure RF distance-bound protocol that verifies the proximity of the key. The solution proposed in [3] includes measuring the signal strength received and determining whether it is from the attacker's device or the key-fob. Measuring the delay is another way to determine if the signal received is from the key or the attacker's device as it will take significantly more time to reach the vehicle. The vulnerability of an attack known as two thief attack in this relay attack scenario has been exposed in [4]. A variety of attempts proposed in [5] to compromise the security of keyless entry systems for automobiles, as well as analysis of various attacks and comparisons of the system's susceptibility to various attacks are provided which gives us an idea of the attack path. The idea of a relay attack is introduced in [6] and distance-bounding methods are examined as a defense and discussion of canonical distance bounding protocols, their relaying mechanisms, and threat modelling are done in depth. An idea for a user context detection method that makes use of multiple sensors to detect the user's location, behaviour, etc. is introduced in [7], which uses an app to collect data from the user's GPS, accelerometer, and then generates a model to determine whether he is in the vicinity of the vehicle or not. The work by authors in [8] contributes to the field of automotive security and highlights the importance of robust cryptographic protocols in keyless entry systems. It raises awareness of potential threats to these systems and emphasizes the need for manufacturers to implement stronger security measures. A proximity detection technique is used to address the relay attack vulnerability by reflecting a signal sent by the car's antenna, and its proximity to the car's antenna is used to determine if the key is within range [9], also analyses the practicality of the system. A defence mechanism is proposed by the authors that uses time stamping and X-or logic as mitigation [10].

Having reviewed the papers, it is found that other published works focus on the mitigations and not on modelling of attack.

The contributions of this paper are:

- This paper introduces MATLAB and Simulink based modelling which gives it a novel approach.
- The modulation and demodulation processes have been elaborated with parameters and component level breakdown.
- Simulation results after each stage have been presented.

3. Problem Formulation

The modern day cars are not only considered as vehicles for commuting, but they are huge information carriers in many forms. They are susceptible to hacking due to advancements in technology. Once the attacker gains access to the vehicle, they can damage or create various attack scenarios. The attack can be carried out quickly without leaving any signs of intrusion. Thus, they pose threats to the security of vehicles as nowadays, vehicles are more connected to various wireless networks. So, to understand the hacker's perspective and approach towards the attack, a relay attack along with proper modelling, simulation, and results have been introduced.

A vehicle manufacturing company outsources its components for design to its suppliers/vendors. Therefore, the knowledge of components and their software incorporated needs to be well known. An elaborate component level analysis is required by manufacturers to justify their design via software simulation for the supplier companies to design the hardware for them, according to which they can estimate the risks associated with the key system and design the mitigations. So, the model and its analysis will help understand the vulnerability of the attack.

4. Working Principle

The relay attack consists of two relay blocks. Relay A is placed near the vehicle which mimics the key-fob while relay B is in the vicinity of the key-fob. Relay A receives the low powered signal from the vehicle, up-converts it to a higher frequency, so that it can travel a larger distance, and then amplifies it. This amplified signal is received by the relay B device which then down-converts it back to its original frequency and transmits it to the key-fob. The key upon receiving this signal sends an authentication message to the vehicle. Since the keys can communicate over a relatively larger distance (30-50 m), the vehicle receives this message and unlocks the door. It is to be noted that this attack does not require any decryption or tampering of the message and hence adding any layer of encryption will not safeguard against a relay attack. The subtopics below explain the architecture of components used in the process along with working.

4.1 Relay A Architecture

The task of the first relay is to receive the incoming signal from the vehicle and boost it to relay B. To do this, we first amplify the signal using suitable LNAs (Low Noise Amplifiers) (as in Fig 2). It is placed as the first component of the transceiver chain to improve the overall noise performance. The signal is then filtered and fed to an up-mixer, of Local Oscillator (LO) frequency 2.4 GHz, for transmission. Bandpass filters are placed to filter the out of band frequencies. The final component used is a power amplifier (PA), to provide sufficient output power to the antenna. The antenna is assumed to be a helical antenna with a gain of 7 dBi.

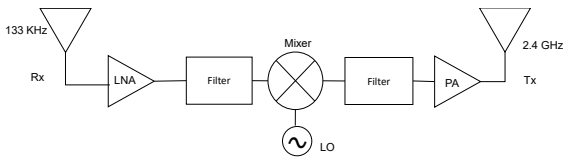

***Fig 2**: Block diagram for Relay A*

4.2 Relay B Architecture

Relay B is placed near the key-fob (about 5-8m). This block receives the up-converted signal, down-converts it and again translates it to the original LF signal of 133 kHz which

is to be received by the key fob (as in Fig 3). The RF chain is similar to relay A, except for the down mixer.

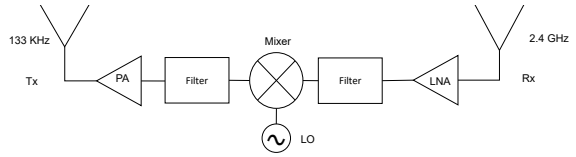

***Fig 3**: Block diagram for Relay B*

4.3 Path loss due to free space channel

The channel has been modelled using the Friis Transmission equation. The path loss component has been assumed for an urban cellular scenario.

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi D}\right)^n \quad \textbf{(1)}$$

Where P_r is the power received by Relay B,
P_t is the power transmitted by relay A,
G_t and G_r is the gain of the antennas,
D is the separation between the two blocks and
n is the path loss component (here n = 2.7 for urban cellular scenario).

5. Simulink Model for Relay Attack

The relay model is made using Simulink and RF Toolbox (as seen below in Fig 4). The RF Budget Analyzer app is used to make the budget link calculations. The input power is considered as -10 dBm. The goal was to design the blocks such that the key-fob receives sufficient power over the distance considered, i.e. 30m.

The parameters of the amplifiers and mixers are chosen based on practical devices. The figures below show the designed RF chain for the relay blocks (Fig 5 and Fig 6). The parameters of the devices modelled are based on off-the-shelf components which are mentioned in Table 1.

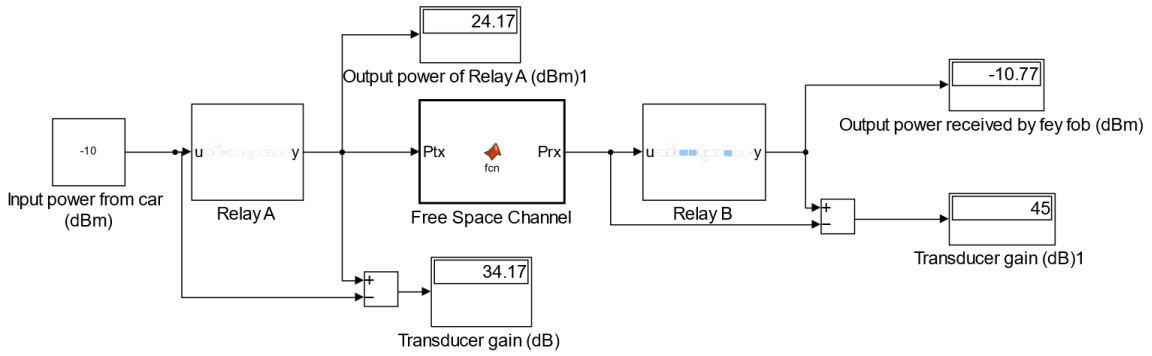

***Fig 4**: Budget Analysis for Relay attack*

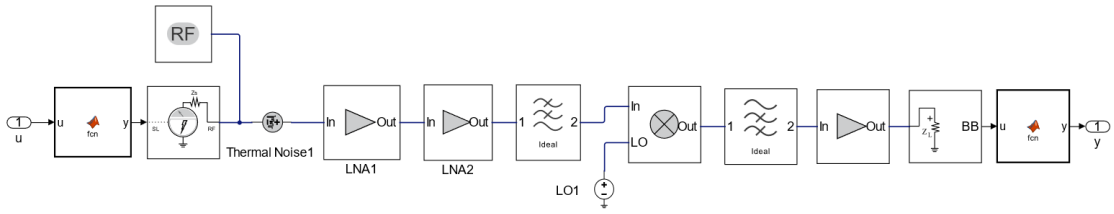

***Fig 5**: Architecture for Relay A*

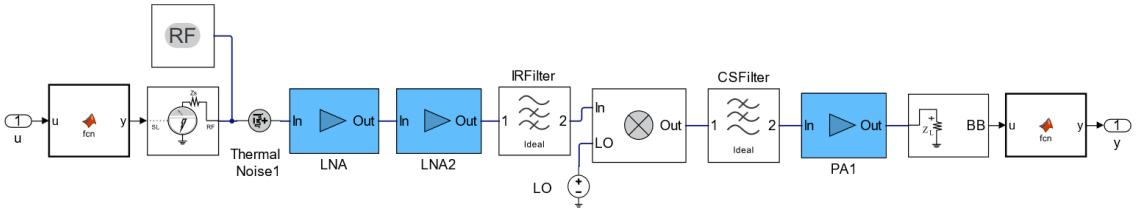

***Fig 6**: Architecture for Relay B*

Table 1: Simulation Parameters

Input power	LNA 1		LNA 2		Mixer		Filter	Power Amplifier		Channel Loss
	NF*	Gain	NF*	Gain	NF*	Gain	Cut-off freq	NF*	Gain	
-10 dBm	1.5 dB	17 dB	1.5 dB	17 dB	7 dB	-7 dB	2.400135 GHz	3 dB	18 dB	80 dB

*NF- Noise Factor, LNA- Low Noise Amplifier

6. Results

The initial power budget calculations show that the output power of relay A after amplification and up-mixing is 24 dBm (as seen in fig 4). After suffering a loss of ~80 dB due to the channel loss, the signal is amplified through relay B and finally transmitted to the key-fob. Upon receiving the signal from relay B, the key fob sends an encoded message to the vehicle, after which the door is unlocked.

To verify the above architecture shown, a MATLAB script has been implemented that mimics the functioning of each block. Initially, an arbitrary signal of frequency 133 kHz to imitate the message signal from the key-fob has been considered. A 2.4 GHz signal has been considered as the Local Oscillator frequency. The two signals were multiplied to modulate the message signal. The modulated signal was multiplied with a suitable constant to mimic the overall gain of the amplifiers. Noise and an interfering signal were added to model the non-linearities of the transmission. A channel loss of 80 dB was introduced to model the path loss. The signal after passing through the loss was received at the input of the relay B. Suitable gain was added to imitate the Low Noise Amplifiers. The demodulation operation was performed and passed through a low pass filter to get back the original message signal. The plots below show the signal at various stages of the transmission chain. A test case has been implemented to verify the functioning of the model using the distance.

As Friis transmission equation suggests, the distance between both the relays plays an important role as far as the attack scenario is considered. The power received by relay B is inversely proportional to the distance between the relays. The plot in Fig 7 represents a 133 kHz random signal which represents the signal from the key fob.

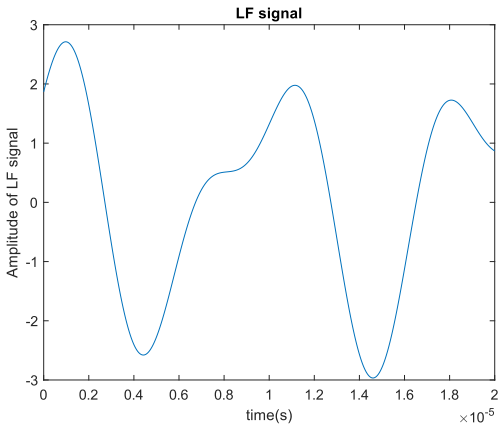

Fig 7: *LF signal vs time(s)*

The signal in Fig 8 represents the message on mixing with the local oscillator signal producing a modulated signal whose frequency is the sum of both input frequencies. Fig 9 shows the relay A signal passing through the free space channel attenuates and undergoes interference. This distorts the signal.

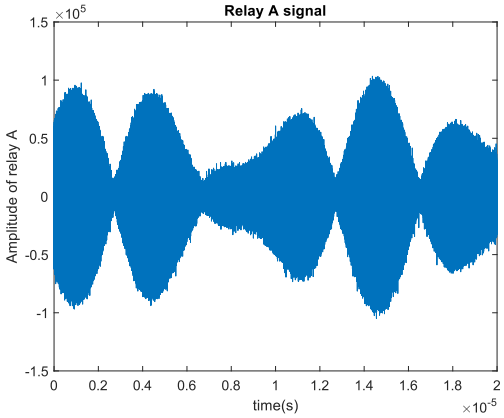

Fig 8*: Relay A signal vs time(s)*

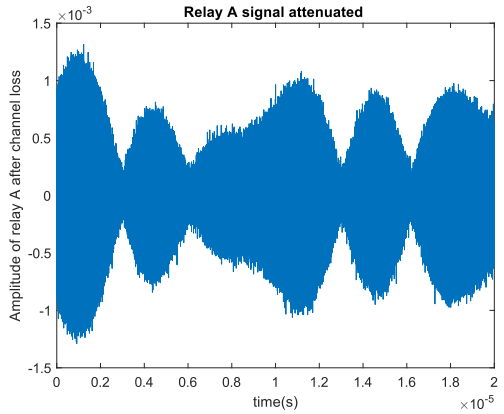

Fig 9*: Relay A signal after channel loss vs time(s)*

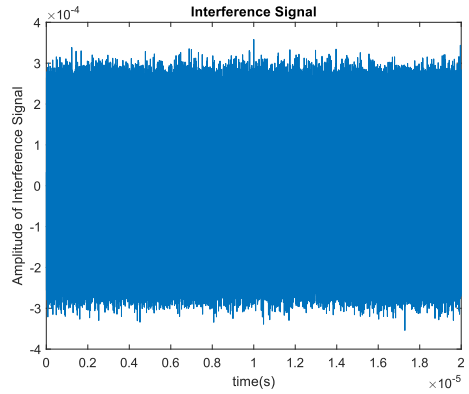

Fig 10*: Interference signal vs time(s)*

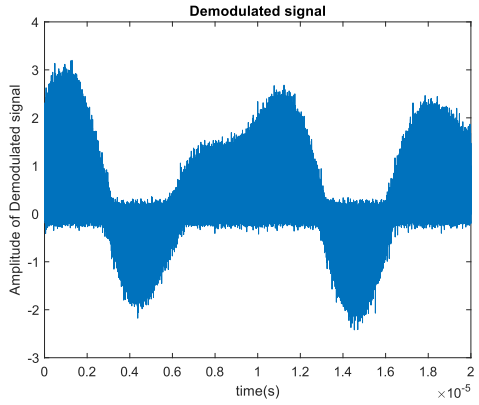

***Fig 11**: Demodulated signal vs time(s)*

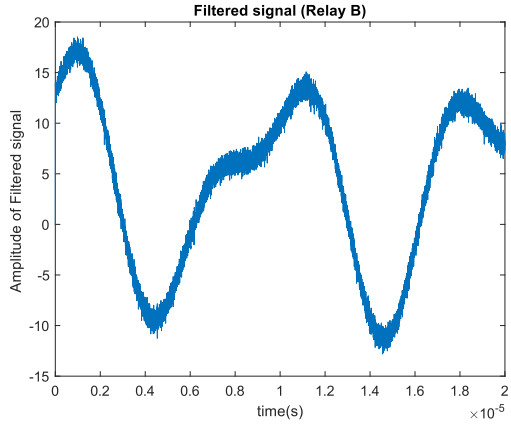

***Fig 12**: Filtered signal vs time(s)*

The signal in Fig 10 imitates a random interference signal. Fig 11 represents the demodulated signal after being subjected to down mixing with the same oscillator frequency.

The demodulated signal on passing through a low pass filter gives back the original message signal as in Fig 12 with a change in amplitude.

According to equation (1), the power received by relay B is inversely proportional to the distance between the relays raised to the power 'n'. Initially, the distance between the relays is considered to be 30 m. At this distance, the path loss is approximately 80 dB. When this distance is reduced to 15 m, the loss reduces to approximately 71 dB. This shows that the output of relay B will have greater signal strength and will be able to unlock the vehicle without the relay B being too close to the key-fob.

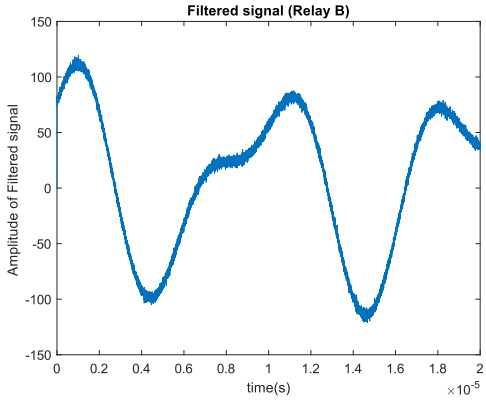

***Fig 13**: Filtered signal vs time(s)*

In this paper, it is found that on reducing the distance (reducing the loss), the amplitude of the signal increases in comparison to the previous case (as in Fig 13). The filtered signal (relay B) gets amplified by almost 10 times as can be seen in the figure. Hence, the signal is faithfully relayed.

7. Conclusion

From the results, it is evident that the relay attack scenario with the proposed MATLAB model has been successfully carried out. The key-fob signal has been relayed over a greater distance faithfully, which would help unlock the car without the knowledge of the owner.

Our purpose here is to make sure that the output signal matches with that of the input. Here, in this case, it is a low frequency signal. The output expected was to be the same signal with an amplified version. The signal is distorted due to the addition of noise and interference as noise is inevitable.

From this, if the distance between the two relay blocks is relatively lesser, then the attacker can place the relay B block farther to the key and still unlock the vehicle as a signal with greater power will be transmitted as seen from the simulation results.

The severity of this attack has been exposed. It is quite important to realize the significance of mitigating this attack as once one gets access to the vehicle, he can get into the Onboard Diagnostic and can perform several attacks such as False data injection or denial of service.

8. References

[1]. Ahmad, U., Song, H., Bilal, A. *et al.* Securing smart vehicles from relay attacks using machine learning. *J Supercomput* **76**, 2665–2682 (2020). https://doi.org/10.1007/s11227-019-03049-4

[2]. Francillon, Aurélien & Danev, Boris & Capkun, Srdjan. (2010). Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.. IACR Cryptology ePrint Archive. 2010. 332.

[3]. Kim, G. , Lee, K. , Kim, S. and Kim, J. (2013) Vehicle Relay Attack Avoidance Methods Using RF Signal Strength. *Communications and Network*, **5**, 573-577. doi: 10.4236/cn.2013.53B2103.

[4]. 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, March 2003, doi: 10.1109/TVT.2003.808759.

[5]. Alrabady, A.I. & Mahmud, S.M.. (2005). Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. Vehicular Technology, IEEE Transactions on. 54. 41 - 50. 10.1109/TVT.2004.838829.

[6]. Avoine, G., Boureanu, I., Gérault, D., Hancke, G.P., Lafourcade, P., Onete, C. (2021). From Relay Attacks to Distance-Bounding Protocols. In: Avoine, G., Hernandez-Castro, J. (eds) Security of Ubiquitous Computing Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-10591-4_7

[7]. Li J, Dong Y, Fang S, Zhang H, Xu D. User Context Detection for Relay Attack Resistance in Passive Keyless Entry and Start System. *Sensors*. 2020; 20(16):4446. https://doi.org/10.3390/s20164446

[8]. Wouters, L., Gierlichs, B., Preneel, B. (2021). "My other car is your car: compromising the Tesla Model X keyless entry system." IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(4), 149-172. DOI: 10.46586/tches.v2021.i4.149-172.

[9]. Park, H.; Hong, J. *BackProx*: Secure Backscatter-Assisted Proximity Detection for Passive Keyless Entry and Start Systems. *Sensors* **2023**, *23*, 2330. https://doi.org/10.3390/s23042330

[10]. K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh and V. Devabhaktuni, "A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic," in *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 101-108, 1 Jan. 2021, doi: 10.1109/MCE.2020.3012425.