A Solution Against Selective Jamming Attack in IEEE 802.15.4e Wireless Networks

Xinlong Wang, Wei Yang(✉), and Chengqi Hou

School of Software, Jiangxi Normal University, Nanchang, China
yw@jxnu.edu.cn

Abstract. Industrial wireless technology plays a crucial role in the application of the Internet of Things (IoT). Among them, in the context of increasingly complex network topologies and the issue of control node energy consumption, the IEEE 802.15.4e protocol is a standard protocol for industrial wireless networks. The protocol incorporates Time Slotted Channel Hopping (TSCH) technology, which is widely adopted in the industrial wireless network domain due to its low latency and high reliability characteristics. However, the IEEE 802.15.4e protocol does not specify a link scheduling algorithm, leaving TSCH networks vulnerable to intelligent jamming attacks. In this paper, we explore the impact of intelligent jamming attacks on TSCH networks and emphasize the harmful consequences of this type of attack. Subsequently, a channel selection scheme for user nodes at the MAC layer of TSCH networks is proposed. Leveraging the background of game theory, the problem of link channel selection is modeled as a Stackelberg game, and a method based on stochastic selection theory is utilized to derive the game solution through the continuously updated probability matrix. Results, considering both system jamming calculations and node transmission rates, demonstrate the high effectiveness and sufficient reliability of the proposed scheme in mitigating selective intelligent jamming attacks.

Keywords: TSCH · Selective jamming attack · Channel selection

1 Introduction

With the rapid progress of science and technology, the application of the Internet of Things (IoT) in industrial wireless networks is receiving increasing attention. The integration of IoT has brought intelligence, automation, and efficiency to industrial devices, production processes, and logistics management, resulting in significant improvements in productivity and management levels for enterprises. In the implementation of IoT applications, industrial wireless technology plays a fundamental and critical role. The IEEE 802.15.4 [1] and IEEE 802.15.4e [2] protocol standards define the requirements for industrial wireless sensor networks at the physical, link, and network layers, ensuring communication quality

Y. Cao and X. Shao (Eds.): DIONE 2023, LNICST 515, pp. 255–262, 2025.
https://doi.org/10.1007/978-3-031-80713-8_19

and reliability. Among these standards, Time Slotted Channel Hopping (TSCH) technology, a core component of the IEEE 802.15.4e standard, is a time-slotted, multi-channel access protocol that provides reliability and stability for industrial applications. TSCH technology can effectively operate in complex wireless environments and high-load conditions while meeting the diverse requirements of different industrial applications in terms of network latency, bandwidth, and data reliability. Many industrial wireless protocol standards, such as Zigbee [3], have adopted TSCH technology to ensure network reliability and stability.

However, the security of industrial wireless networks has always been an unavoidable issue, with new challenges arising from intelligent communication jamming, such as those initiated by unmanned aerial vehicles (UAVs). TSCH technology employs a fixed channel selection method, allowing UAVs to monitor the channel used by nodes during their communication time slots and launch intelligent jamming during subsequent communication intervals. Given that TSCH technology utilizes periodic slot allocation, when UAVs initiate intelligent jamming attacks, the performance of industrial wireless networks will be severely affected, including increased data transmission latency, communication link interruptions, and even potential network system crashes.

In response to the network security vulnerabilities mentioned above, many scholars have proposed corresponding solutions. Kang et al. [4] employed spatial retreat techniques in the field of unmanned aerial vehicles (UAVs) to achieve resilient networks and optimize security solutions. This article solves the problem of traditional unmanned aerial vehicles being prone to communication failures in poor channel conditions. The CSR algorithm in the article estimates the jamming center point based on position information, thereby changing the channel scheme at the physical layer. Article [5] proposed a security-aware batch processing MAC layer protocol for secure channel allocation. This scheme utilizes the parallel transmission capability of the CR-IoT device to improve network performance and also has the ability to perceive interference. In terms of channel allocation, it is transformed into a binary linear programming problem. In [6], an enhanced blacklist-based solution was presented to enhance the TSCH protocol. The proposed algorithm models channel quality estimation as a multi arm slot machine problem to improve the frequency hopping spread spectrum strategy and avoid selecting low-quality frequencies. The aforementioned solutions based on the physical layer require certain hardware support and system deployment, often having limitations in dynamic interference environments. On the other hand, solutions at the link layer only address single-channel scenarios, suitable for solving single-hop problems but not applicable to multi-channel environments in TSCH networks. Drones can monitor the timeslot channels during node communication and intelligently interfere with the subsequent communication moments, causing disruptions and security threats to the network. This intelligent interference may lead to increased data transmission delays, communication link interruptions, or even system crashes. The TSCH protocol employs a periodic time slot allocation method, which is vulnerable to disruption attacks, significantly impacting the performance of industrial wireless networks. Many

proposed solutions in academia for intelligent interference attacks, including spatial retreat techniques, security-aware MAC layer protocols, blacklist approaches, often require specific hardware support or have certain limitations, especially in dynamically changing interference environments. This paper, based on the attack node's periodic interference selection model, introduces a channel selection approach at the link layer under the background of game theory, taking into account the situation of multi-channel frequency hopping, to optimize the solution for the channel hopping problem.

This paper is based on the IEEE 802.15.4e protocol and will introduce the characteristics and steps of selective jamming attacks in Sect. 2. In Sect. 3, a channel selection scheme is proposed to address selective jamming attacks. The proposed scheme is evaluated through simulation experiments in Sect. 4, comparing its performance with different schemes. The results demonstrate the strong effectiveness of the strategy proposed in this paper. Finally, Sect. 5 provides a summary of the proposed solution.

2 Selective Jamming Attack

Selective jamming attacks are a type of attack targeting TSCH (Time Slotted Channel Hopping) networks with the aim of disrupting communication and coordination within the network. Attackers first monitor the TSCH network to gather information about its topology, communication frequencies, slot arrangements, and other relevant details. This can be achieved by eavesdropping on network traffic, observing interactions between nodes, and analyzing data packets transmitted within the network. During the monitoring phase, the attacker selects one or more target nodes for the attack. These target nodes are often critical or control nodes within the network, and compromising or disrupting them would have a significant impact on the overall network operation. Once the target nodes are selected, the attacker employs jamming devices or specially crafted wireless devices to transmit intentionally disruptive wireless signals towards the target nodes. These disruptive signals may include noise, interference waveforms, or malicious data packets, all aimed at disrupting the communication and coordination processes of the target nodes. The attacker monitors the responses of the target nodes and observes the behavior of the network, making adjustments to the interference signal's intensity, frequency, or pattern as needed. Through continuous monitoring and adjustment, the attacker maximizes the interference on the target nodes, thereby impacting the performance and stability of the entire TSCH network.

3 Channel Selection Scheme Based on Stackelberg Game

In the following, we will model both the attacker and the victim node, propose a channel selection scheme based on Stackelberg game.

The model consists of N user nodes and 1 selective jamming node. Taking the mesh topology structure in Fig. 1 as an example, which includes 5 user

nodes, i.e., $N = 5$, we define the set of users as $\mathbb{N} = \{1, 2, 3, \ldots, N\}$, and the set of channel selections as $\mathcal{M} = \{1, 2, 3, \ldots, M\}$. In this system model, the selective jamming node can obtain the channel selection sequence used by the user nodes before detecting jamming and sequentially enter channels to attack nodes, maximizing its jamming utility. On the other hand, users, upon observing the actions of the jamming node, continuously update their defense strategies by changing their channel selections to reduce the success rate of the jamming attacks.

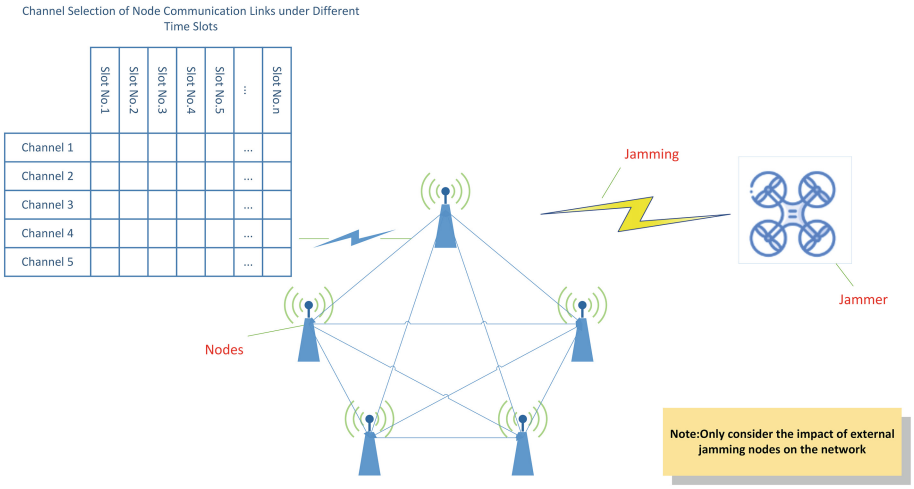

Fig. 1. Network Model.

Strategy sets are created for both the user nodes and the jamming node. Let $a_u = \{a_1, a_2, \ldots, a_n\}$ and $a_j = \{a_{n+1}, a_{n+2}, \ldots, a_{2n}\}$ represent the channel selection strategies for the user nodes and the jamming node, respectively, where n represents the number of elements in the node's link channel sequence set. When both the user nodes and the jamming node select the same channel strategy, i.e., $a_i = a_{i+n} (i \in [1, n])$, jamming attacks are executed, resulting in transmission jamming. The model considers the scenario of block fading [7] in data transmission, where the channel gain of nodes changes when the channel selection changes. We choose to consider the Rayleigh fading model, and define the channel gain for user m transmitting data to user n as:

$$H_{mn}^{a_n} = \beta_{mn}^{a_n} * (d_{mn})^{-\alpha_1} \tag{1}$$

where a_n, $\beta_{mn}^{a_n}$, d_{mn}, and α_1 represent the channel strategy chosen by user m, the path fading coefficient, the distance between user m and user n, and the path fading exponent, respectively. Similarly, we define the channel gain for jamming node j transmitting data to user n as:

$$H_{jn}^{a_j} = \beta_{jn}^{a_j} * (d_{jn})^{-\alpha_2} \tag{2}$$

where a_j, $\beta_{jn}^{a_j}$, d_{jn}, and α_2 represent the channel strategy chosen by jamming node j, the path fading coefficient, the distance between jamming node j and user n, and the path fading exponent, respectively. In TSCH networks, due to the use of frequency hopping, different nodes communicate using different hopping channels in different timeslots, thus avoiding co-channel interference between nodes. In this paper, we only consider the impact of external jamming nodes on the network. The jamming experienced by user n is defined as:

$$J_n = P_j * H_{jn}^{a_j} * f(a_j, a_n) \tag{3}$$

where P_j is the transmission power of the jamming source, and the indicator function can be represented as $f(x,y) = \left\{ \begin{array}{l} 1, x = y \\ 0, x \neq y \end{array} \right\}$,indicating that jamming occurs when user nodes and jamming nodes select the same channel, and no jamming occurs otherwise. Based on this, we can formulate the expected jamming (EJ) formula for the system model as:

$$EJ = \sum_{i \in n} P_i * P_j * \bar{H}_{ji}^{a_j} * f\left(a_j, a_i\right) \tag{4}$$

where $\bar{H}_{ji}^{a_j} = E\left[H_{ji}^{a_j}\right] = \bar{\beta}_{ji}^{a_j} * \left(d_{ji}\right)^{-\alpha_2}$ represents the expected value of the channel gain. Our objective is to minimize the EJ in order to achieve effective jamming resistance through an optimized channel selection scheme. Therefore, the optimization objective of the system can be formulated as:

$$(P_1) : S_{opt} = \arg\min EJ = \arg\min \sum_{i \in n} P_i * P_j * \bar{H}_{ji}^{a_j} * f\left(a_j,\ a_i\right) \tag{5}$$

The transmission rate of user node n can be expressed as:

$$R_n = B \log_2 \left(1 + \frac{P_n \bar{H}_{nn}^{a_n}}{BN_0 + J_n}\right) \tag{6}$$

where B is the channel bandwidth, N_0 is the noise power spectral density, J_n represents the jamming from the attacking node to user node n, and $\bar{H}_{nn}^{a_n}$ denotes the average channel gain of user n.

Next, we construct a Stackelberg game for the aforementioned problem using the set $\mathcal{G} = \{i,\ \mathcal{J},\ a_u,\ a_j,\ u_i,\ u_j\}$ to summarize the game elements. The internal elements represent user nodes, jamming nodes, user node strategy sets, jamming node strategy sets, user node utility functions, and jamming node utility functions, respectively. Assuming that jamming nodes act as leaders and user nodes act as followers.

For jamming nodes, their objective is to maximize the effectiveness of jamming by implementing specific strategies. Their utility function can be defined as $u_j\left(a_n,\ a_j\right) = \sum_{i \in n} P_i * P_j * \bar{H}_{ji}^{a_j} * f\left(a_j,\ a_i\right)$, and the corresponding optimization problem is expressed as:

$$(P_2) : J_{opt} = \arg\max u_j(a_n,\ a_j) \tag{7}$$

In the utility function, the selective jamming node's monitoring and inference of channels are designed to make the value of the indicator function f equal to 1, thereby maximizing the effectiveness of the jamming strategy.

For user nodes, their objective is to minimize jamming by avoiding the channel selections made by jamming nodes based on data analysis. Their utility function can be defined as $u_n\left(a_n,\ a_j\right) = L - \sum_{i \in n} P_i * P_j * \bar{H}_{ji}^{a_j} * f\left(a_j,\ a_i\right)$, where L represents a fixed parameter that ensures the utility function of user nodes is always greater than 0. The corresponding optimization problem is expressed as:

$$(P_3) : N_{opt} = \arg\max u_n(a_n,\ a_j) \tag{8}$$

In the utility function, user nodes aim to avoid the channel selections made by selective jamming nodes in order to solve the optimization problem and minimize jamming. They strive to make the value of the indicator function f equal to 0, thereby maximizing the effectiveness of the defense strategy.

We choose a method based on random selection theory to solve the equilibrium solution of the game problem $\mathcal{G}$. The update cycle of selective interference nodes is defined as one Epoch, each containing one superframe experienced by the link transmission. Selective interference nodes continuously update channel selection strategies among k Epochs by monitoring the network environment. The user node completes the update channel strategy in the superframe timeslot of each Epoch, which references the method of random theory and creates a probability matrix for the user $\theta_{nc}(t)$ provides data support for policy selection, which does not require information exchange between nodes and has been widely used in decision-making problems in wireless communication systems. Assuming the channel selection set is complete, the overall process of the algorithm is as Algorithm 1.

Algorithm 1: Random Theory Method

$t = 0, k = 0, \theta_{nc}(t) = \frac{1}{|len(\mathbb{C})|}$;
$a_j = a_j(k)$;
for t *in* k **do**
    $a_n\left(t\right) = \arg\max \theta_{nc}(t)$;
    $u_n(t)$;
    if $c == a_n\left(t\right)$ **then**
        $\theta_{nc}\left(t+1\right) = \theta_{nc}\left(t\right) + b_1 * \left(\frac{u_n(t)}{L}\right) * \left(1 - \theta_{nc}(t)\right)$;
        else
            $\theta_{nc}\left(t+1\right) = \theta_{nc}\left(t\right) - b_1 * \left(\frac{u_n(t)}{L}\right) * \theta_{nc}(t)$;
            //B_1 represents the learning step size, satisfying $0 < b_1 < 1$;
$k = k + 1,\ to\ 2$;
//The algorithm terminates when the preset k value is reached.

4 Performance Analysis

In this section, we present the results of the proposed solutions for selective jamming and compare the effectiveness of different defense strategies. We design five channels for the simulation. The transmission powers of the user nodes and jamming nodes are set to P_n=2W and P_j=25 W, respectively. The path loss exponent is set to $\alpha = 2$, the learning step size is set to $b_1 = 0.02$, the fixed parameter is $L = 0.07$, the channel bandwidth is $B = 1$ MHz, and the noise power spectral density is $N_0 = -100$ dB/Hz.

To evaluate the effectiveness of the proposed method, we consider two metrics: the Expected Jamming value (EJ) and the user node's transmission speed (TS). Figure 2 compares three scenarios: using the proposed defense strategy, using a random channel selection strategy, and having no anti-jamming strategy. In this comparison, we assume that the channel communication quality is ideal, and all jamming is caused by external selective jamming attacks.

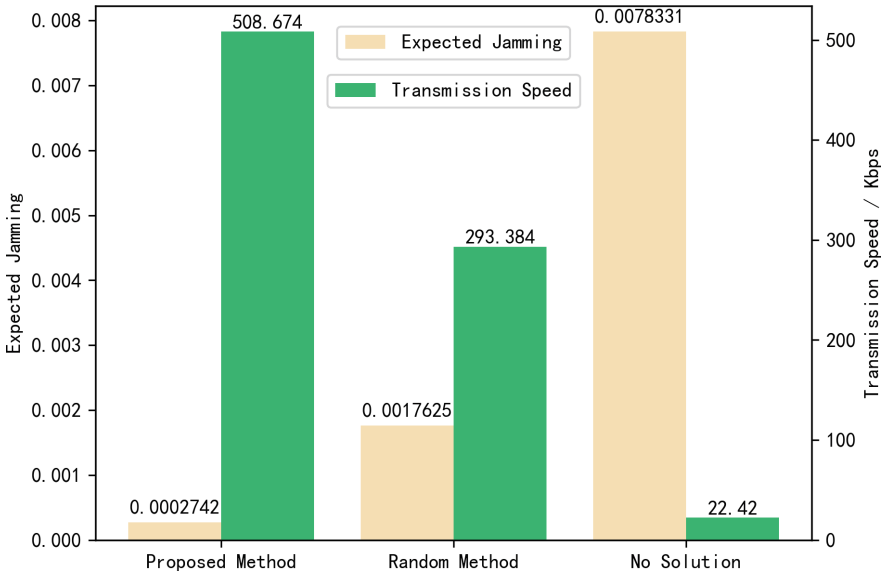

Fig. 2. Comparison of system's expected jamming(EJ) and node's transmission speed(TS) under different defense strategies.

In 200 epochs, we calculated the average value of the system's expected jamming(EJ). Each epoch consists of 5 user channel decisions, and when the user node's strategy matches the jamming node's strategy, the average value of the EJ increases. As shown in Fig. 2, our proposed method reduces the EJ value by 24 times compared to having no solution and 5 times compared to the random channel selection scheme. In each epoch, for every 1 mistake made in the user node's decision, the EJ value increases by 0.0015666. In other words,

out of 1000 decisions in 200 epochs, our proposed method avoids 959 incorrect decisions compared to having no solution and 165 incorrect decisions compared to the random channel selection scheme. In terms of transmission speed(TS), thanks to fewer attacks from jamming nodes, the average TS of user nodes in our proposed solution reaches 593.097 Kbps, which is 26 times and 2.2 times higher than having no solution and the random channel selection scheme, respectively. Therefore, our proposed solution demonstrates high effectiveness in addressing intelligent jamming attacks.

5 Conclusion

This paper proposes a defensive anti-jamming strategy against selective intelligent jamming attacks in industrial wireless networks. The proposed solution is based on IEEE 802.15.4e TSCH networks and utilizes channel hopping for node's channel selection strategy. The problem is modeled as a Stackelberg game and the equilibrium solution is obtained using stochastic learning theory. In the simulation experiments, based on the changes in the probability matrix, user nodes are able to select the optimal channels for data transmission, successfully avoiding the channel selections of intelligent jamming nodes. The experimental results demonstrate the high effectiveness of this approach.

Acknowledgments.. This work is supported by the National Natural Science Foundation of China under Grant No.62002143 and the Natural Science Foundation of Jiangxi Province under Grant No. 20224BAB202011.

References

1. 802.15.4-2007: IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs): Amendment 1: Add Alternate PHYs. IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006), 1–210 (2007)
2. 802.15.4e-2012: IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer. IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–225 (2012)
3. Zigbee Homepage. https://csa-iot.org/zh-CN/developer-resource/specifications-download-request. Accessed 30 May 2023
4. Kang, J., Kwon, Y., et al.: Cooperative spatial retreat for resilient drone networks. Sensors (Basel) **17**(5), 1424–8220 (2017)
5. Salameh, H.B., AL-Quraan, M.: Securing delay-sensitive cr-iot networking under jamming attacks: parallel transmission and batching perspective. IEEE Internet Things J. **7**(8), 7529–7538 (2020)
6. Gomes, P.H., Watteyne, T., et al.: MABO-TSCH: multi-hop and blacklist-based optimized time synchronized channel hopping. Trans. Emerg. Telecomm. Technol. **29**(1), 1–15 (2018)
7. Bistritz, I., Leshem, A.: Game theoretic dynamic channel allocation for frequency-selective interference channels. IEEE Trans. Inf. Theory **65**(1), 330–353 (2019)