Evaluation of Channel Hopping Strategies Against Smart Jamming Attacks

Emilie Bout, Valentin Bout, Alessandro Brighente, Mauro Conti, Valeria Loscri

Evaluation of Channel Hopping Strategies Against Smart Jamming Attacks

Emilie Bout
Inria Lille- Nord Europe
Lille, 59000 France
emilie.bout@inria.fr

Valentin Bout
University of Lille
Lille, 59000 France
valentin.bout.etu@univ-lille.fr

Alessandro Brighente
University of Padova
Padova, 35100 Italy
alessandro.brighente@unipd.it

Mauro Conti
University of Padova
Padova, 35100 Italy
mauro.conti@unipd.it

Valeria Loscri
Inria Lille- Nord Europe
Lille, 59000 France
valeria.loscri@inria.fr

***Abstract*—Channel hopping is a well-known methodology to dynamically allocate frequency resources to nodes in wireless communication systems. The aim of channel hopping is to mitigate possible interference issues caused by both legitimate and malicious users. The stateof-the-art channel hopping-based jamming mitigation techniques are becoming increasingly smart by using game theory or machine learning. However, we show in this paper that, although the victim may employ smart channel hopping strategies, these are not always effective in mitigating attacks.**

In this paper, we implement an effective jamming attack strategy to impair the effectiveness of channel hopping mitigation strategies. We test our attack on a testbed network composed by real devices, and test its effectiveness against three mitigation strategies: i) incremental channel hopping, ii) random channel hopping, and iii) smart channel hopping. We show that, by implementing our attack, an attacker can reduce the number of successfully transmitted packets by at least 28.5%, even against the smart channel hopping strategy.

***Index Terms*—Channel Hopping Methods, Jamming Attacks, Wireless Networks**

I. Introduction

Wireless networks have enabled the development of new communication paradigms, including cellular networks and the Internet of Things (IoT). However, due to the openness of the wireless medium, these new paradigms present new challenges in terms of resource allocation, interference management, and novel attack strategies. To deal with these challenges, several wireless communication protocols envision the use of different frequency bands for communications, and each frequency band is separated into channels. Exploiting this paradigm, *channel hopping* has been proposed to regularly or adaptively change the communication channel assigned to nodes in the network to limit both collisions and interference generated by neighboring devices. Several standard network protocols use channel hopping methods, with examples such as 802.15.4 protocol with the Time Slotted Channel Hopping (TSCH) or Bluetooth with the Frequency Hopping Spread Spectrum (FHSS) and Adaptive Frequency Hopping Spread Spectrum (AFH) [1]. We also find channel hopping methods in cognitive radio to avoid noise effects and improve the control channel saturation problem [2]. Finally, these solutions are also employed in propriety protocols, such as that used for DJI drones where FHSS is one of several integrated methods [3]. Besides resource allocation, channel hopping allows to mitigate the effects of several attacks. Indeed, attackers face more difficulties in intercepting communications when they dynamically occur on different channels. This is the case for passive attacks such as eavesdropping, where the attacker's aim is to steal sensitive users' information by listening to packets. Active attacks instead imply interactions between the attacker and the communications originating from the victim. Examples of such attacks include denial of service attacks via *jamming*, which limits the operation of a target victim device.

The literature proposes many strategies to select the future communication channel. This ranges from basic algorithm, e.g., pseudo-random channel selection, to advanced machine learning methods using real-time network characteristics. Indeed, in recent years researchers developed a new category of "smart" channel hopping approaches, being more autonomous, more adaptive, and more efficient than basic ones. In [4], the authors simulate and evaluate nine methods based on Multi-Armed Bandit (MAB) algorithms to solve the problem of selecting the best channel to transmit in 802.15.4-TSCH Networks. They conclude that Thompson sampling algorithm is one of the fastest to converge to the optimal channel and this hypothesis is also validated with real experiments in [5]. A Q-Learning algorithm to approach the optimal channel hopping pattern is investigated in [6] against probabilistic jamming. The authors show that, without prior knowledge of the jamming model, the developed algorithm can find a feasible channel hopping strategy with good performance and fast convergence.

Along with smarter defense, also attackers' strategies are becoming more and more elaborate to circumvent new mitigation systems. Indeed, the authors in [7], propose a new

This work was partially supported by a grant from CPER DATA and by the General Armament Direction, France and the Defense Innovation Agency, France.

optimal attack based on an integer programming problem and validate it via simulation to counter a proactive channel hopping method. In [8], an intelligent selective jamming attack was established against a Wireless-Hart network. By doing passive listening, the authors were able to deduce the TSCH channel hopping sequence. The authors in [9] proposed a game-theoretic approach, where both the attacker and the victim choose the successive channel solving for the optimal strategy. However, authors resolved to Q-learning to compute the solution of the game, hence requiring periodical learning phases that limit the effectiveness in time of the attack. In our previous work [10], we implement an attacker scheme that does not need to periodically stop the attack to learn the new victim's channel hopping strategy, and prove its effectiveness and superiority compared to other attack models. However, its effectiveness and lightweight property were only proven via numerical simulations, not taking into account real-world constraints.

In this paper, we validate our intelligent jamming attack by implementing it on a real testbed. During our previous simulations, certain essential characteristics related to the operation of a network could not be taken into account. For instance, disturbances caused by neighboring networks are not considered by the NS-3 simulator. Therefore, to prove the feasibility of the approach established in [10], we decided to develop it into a test-bed. We evaluate its effectiveness against several channel hopping strategies existing in communication protocols. Moreover, as one of the major points of our algorithm was its lightweight execution, it was important to prove it in reality. We also extend our analysis further by evaluating this attack against a smart channel hopping method. We show that although these defense methods perform well in simulation, in reality they suffer significant weaknesses. Indeed, even if the access point uses a smart algorithm in order to perform channel hopping, the attacker manages to drop the Packet Delivery Ratio (PDR) from 88.7% to 60% when launching the attack.

The main contributions of our work can be summarized as follows.

- We adapted a smart jamming attack that, without needing prior knowledge on the victim's behavior, has the ability of directly learning the victim's channel hopping strategy from real-time channel measurements. Compared to our previously proposed theoretical work [10], in this paper we provide a real testbed implementation and validate the attack based on a richer set of evaluation metrics.
- We implement on our testbed different state-of-the-art channel hopping strategies, namely i) incremental channel hopping, ii) random channel hopping, and iii) smart channel hopping and test our smart jamming attack against them.
- Thanks to our testbed implementation, we provide insights on the use and needs of channel hopping both in case of no attack and smart jamming attack.

The rest of the paper is organized as follows. In Section II, we present the different parts of the network. In Section III we evaluate the effectiveness of several channel hopping strategies against a smart jamming attack. In Section IV the communication performances of the considered scenarios are discussed. Finally, we conclude the paper in Section V.

II. Evaluation Approach

In this section, we describe our evaluation methodology. First, we describe the attacker model. Then, we present the testbed we set up to assess the robustness of the various channel hopping schemes against our new smart jamming attack.

A. Attacker model

The purpose of jamming attacks is to deliberately interfere with a transmission medium in order to corrupt as many packets as possible or interrupt the communication. As an attacker can only jam one channel at a time, channel hopping has proven to be a successful solution to mitigate jamming. However, if the attacker has the ability to learn the frequency hopping pattern, this mitigation method loses its effectiveness.

In this scenario, we develop an attack having the ability to fast converge to the optimal jamming channel. To be effective against channel hopping, the attack must be i) as reactive as possible, and ii) continuous over time. We hence base our strategy on an algorithm that does not require any specific assumptions and can learn online: a Multi-Armed Bandit (MAB) algorithm. Several MAB algorithms have been implemented on the defense side in the literature [4], [5]. In this paper, we adapted them for the attacker's perspective. The complete algorithm of the attacker process is available in our previous paper [10]. We present our proposed attacker's workflow in Fig. 1.

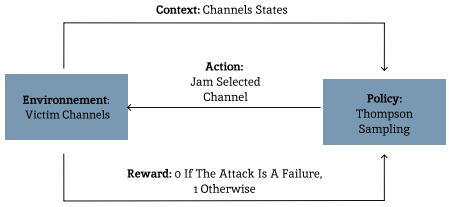

Fig. 1: Attacker Workflow

In MAB algorithms, at each iteration, an agent acts on the environment according to a predefined policy and receives a reward. The goal is to select a policy able to maximize the sum of rewards. In this context, our agent is the attacker and the environment corresponds to the utilization state of the victim's channel, i.e., busy or idle. In [4], [5], the authors experiment several policies for MAB algorithms and conclude that the Thompson Sampling algorithm converges faster than other known methods such as Upper Confidence Bound (UCB) to the optimal channel. Based on these assumptions and after testing algorithms ourselves, we draw the same conclusion. Consequently, at each time step, the attacker executes the Thompson Sampling algorithm to choose the channel to jam

according to the environment and the previous rewards. If the attacker is on the same channel as the victim, the jamming attack is successful, having consequences on the Data Link and Physical layers. Therefore, when the attacker has an effect on the legitimate channel, the Received Signal Strength Indicator (RSSI) of the receiver decreases. In this case, if the receiver's RSSI is below a certain predefined threshold, the attack is considered a success and the reward obtained is equal to 1. Indeed, the attacker knows the RSSI of the channel where the access point is located by scanning packets on the channel. If unsuccessful, the returned reward is 0. Finally, the attacker updates the policy based on the previous observation-action-reward tuples.

B. Victim model

The victim possesses a mitigation approach against jamming attacks, i.e., a channel hopping method. The victim has a predefined set of M channels to use, which can be identified via integer numbers. We evaluated our attack against three different channel hopping implementations: incremental channel hopping, random channel hopping, and a smart channel hopping.

- **Incremental Channel Hopping** ($T_{\text{Incremental}}$): At each defined time, the legitimate nodes on the network increment their channel number by 1. Therefore, the legitimate network nodes follow a well-defined pattern.
- **Random Channel Hopping** (T_{Random}): In order to reduce the chances of inferring the predefined channel hopping pattern, the second method we implemented is a randomness-based method. The master node randomly chooses a new channel among the *M* available and informs the other nodes.
- **Smart Channel Hopping** (T_{Smart}) The method follows the model proposed by the authors in [4], [5] and employs a MAB approach. The objective is to converge to the best channel available in as few steps as possible by employing a Thompson sampling formulation.

C. Network model

We implement a testbed consisting of three legitimate nodes: a transmitter, a receiver, and an Access Point (AP), as shown in Fig. 2. The attacker is equipped with an *Alfa AWUS036h* device and connected to a Raspberry-Pi. We choose this type of instrument to directly modify the MAC layer parameters. Indeed the driver and firmware of the Atheros WiFi chipset are open-source and the are easily extensible. We modify the *hostapd* open source code on the AP side to encode several channel hopping methods not available in the basic protocol such as Smart Channel Hopping. As the distance between the elements of the network plays an important role in the transmission time of a packet, this parameter remains fixed throughout the simulations. The transmitter and the receiver are placed at 1 meter each from the access point and the attacker at 5 meters.

We run experiments over a 6 minutes time frame. At the 30th second, the attenuation method begins to operate, then

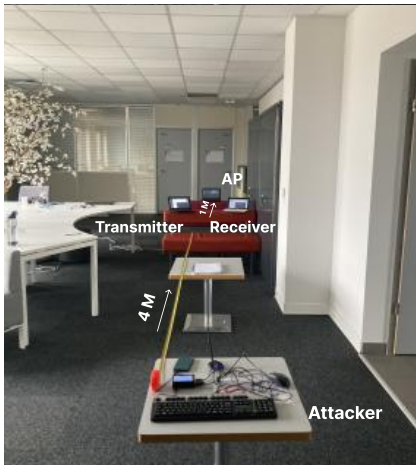

Fig. 2: Testbed implementation

30 seconds later the attacker starts to jam. Each experiment was repeated 5 times and the results presented below are an average of these with a 95% confidence interval. In this study, we set the total number of retransmissions for a packet to 1. So, if a packet has never been received, the transmitter has the option of retransmitting the packet once. For the basic channel hopping methods, the time between each hop was fixed at 0.5 seconds.

III. Performance Evaluation

In this section, we evaluate our new strategy in two scenarios. In Section III-A, we consider a victim using basic channel hopping, i.e. incremental or random channel hopping. Then, in Section III-B we push our evaluation further by taking into account a victim exploiting the aforementioned smart channel-hopping strategy. For these two cases, we compare the different strategies in terms of a) Packet Delivery Ratio (PDR), b) number of retransmissions, c) packet Inter arrival Time (IaT). In order to calculate the PDR on the sender side, we use the TCP-IP protocol to evaluate the success of the transmission with the acknowledgment packets. To estimate the impact of our attack, we use the PDR metric, well known in the literature to identify jamming attacks [11]. The PDR is computed as follows:

$$\text{Packet Delivery Ratio} = \frac{\sum \text{Number of PSD}}{\sum \text{Number of PT}}, \qquad (1)$$

where PSD is the sum of packets successfully received at the destination and PT represents the sum of packets transmitted by the source.

A. Basic Channel Hopping Methods

Fig. 3 shows the impact of our attack on the network considering the PDR evolution over time. We notice that the PDR remains high when no attack takes place. Indeed, after 6 minutes of experiments, the PDR is around 97.8% using the random channel hopping strategy. The same behavior is also

achieved via incremental channel hopping, where the PDR remains above 95%.

Unlike the simulations, the experiments were carried out in a real environment, i.e. in the presence of other neighboring networks. Indeed, we noted the presence of 14 other access points present in the building and certain channel had a high and variable occupancy rate depending on their use over time. Thus, contrary to the simulator where each channel was occupied only by the evaluated communication, in the real environment, the channels undergo natural interference linked to neighboring networks. This behavior is visible by the drop of the PDR. When the attack takes place, the PDR drops dramatically when considering incremental channel hopping. Indeed, due to the victim's periodical pattern, our attacker can efficiently predict the victim's future channel. Consequently, at the end of the experimentation, the PDR is around 31%. On the other hand, when the victim is less predictable thanks to random channel hopping, we notice that our attack still impacts the PDR. Indeed, our smart attacker manages to drop the PDR by 51.62%, being hence effective in the victim's channel prediction. One of the visible effects of jamming attacks is also an increase in the number of retransmissions. Indeed, with certain protocols such as TCP-IP, packets that are malformed or that are not acknowledged have the possibility of being retransmitted. Tab. I shows the number of victim's retransmissions both in presence and absence of the attack. Without attack, the number of transmitted packets is equal to 647.5 and 648.75 for incremental and random channel hopping, respectively. The number of retransmission is low for both cases, around 10. However, when the attack is executed, the number of retransmissions increases dramatically. Indeed, for both cases, the number of retransmitted packets undergoes a ten-fold increase compared to the cases without the attack. As seen previously, the jamming attack impacts communication also in terms of total number of packets sent. Indeed, the number of packets sent is halved when victim follows the incremental channel hopping strategy.

The effect of this smart attack on basic channel hopping strategies is also visible in terms of packet IaT. Fig. 4 shows the IaT for the two basic channel hopping methods. As we observe in the figure, the average packet inter arrival time is equal to 2.43 seconds with the incremental channel hopping method and 2.16 seconds with the random channel hopping method. In both cases, at a given time, the arrival time between two packets can exceed 5 seconds, which corresponds to the effect of a successful jamming attack. It can be hence deduced that the attacker occupies the same channel as the victim at the same time.

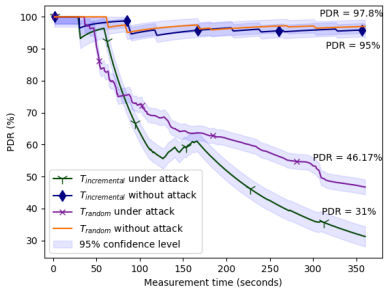

Fig. 3: PDR for different basic channel hopping defense strategies against smart attacks

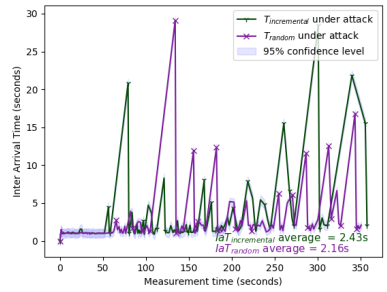

Fig. 4: IaT for different basic channel hopping defense strategies against smart attacks

Tab. II, summarizes the accuracy of the smart jammer model according to several strategies of channel hopping. The accuracy of the attack is computed as follows:

$$\text{Accuracy} = \frac{\sum \text{Number of GA}}{\sum \text{Number of TA}}, \tag{2}$$

where GA denotes good actions taken by the attacker and TA corresponds to the total action in terms of number of packets taken by the system.

Type	Accuracy(%)
Incremental Channel Hopping	82% (+/- 4 %)
Random Channel Hopping	75.6% (+/- 2 %)
Smart Channel Hopping	65.2% (+/- 7.2 %)

TABLE II: Accuracy of the jamming model against different channel hopping methods.

The results for the incremental and random channel hopping methods confirm the inefficiency of these solutions. Indeed,

	Without Attack		Under Attack	
Type	**Number of packets**	**Number of retransmissions**	**Number of packets**	**Number of retransmissions**
Incremental Channel Hopping	647.5	10.5	365.75	114.75
Random Channel Hopping	648.75	9.75	403	107.66
Smart Channel Hopping	552.6	47.33	480.4	89.85

TABLE I: Number of retransmissions for different channel hopping strategies without and under attack.

after 5 minutes of attack, the model has an accuracy of 82% and 75.6% for the incremental and random channel hopping, respectively.

The simulations carried out in the paper [10] had proven that this type of attack was effective against basic channel hopping methods. The experiments confirmed this result and the feasibility of our approach in lightweight devices.

B. Smart Channel Hopping Methods

To further validate the effectiveness of our attack, we test it against a victim having the ability to react according to the sensed environment. The channel hopping strategy also employs a MAB algorithm with a Thompson Sampling method as described in [5]. The victim's reward is calculated on the access point side and it is based on two metrics: the PDR, and the number of nodes lost after the channel change. As previously discussed, both the presence of other networks and the jamming attack impact on the PDR. Additionally, if a jamming attack has already taken place on another channel, and the access makes the wrong decision and orders other network nodes to go to that channel, communication cannot be reestablished because the nodes will be under attack. Therefore, as we are in a real environment and other communications take place in parallel, we set the detection threshold of the PDR to 60%. As our experienced network is composed by two nodes, the threshold on the number of connected nodes is defined at 1. Consequently, if the PDR is less than 60% and the number of connected nodes less than 1, the environment returns 0 as a reward to our AP, which updates its policy with this information. The behavior of the PDR obtained after 6 minutes of experimentation with and without attack is shown in the Fig. 5. Surprisingly, without attack the PDR at the end of the experimentation is around 88.7%, which is 6.3% less than with basic channel hopping methods. This can be explained by the fact that our victim initially explores several times all the channels before converging to the optimal solution. However, as already mentioned above, during experimentation, natural interference causes collisions and additional retransmissions during the exploration phase. This convergence time causes the PDR to drop during the first stage which is represented on the curve between the timestamps 30 and 80 seconds. Then, the algorithm converges to the optimal solution and manages to maintain a stable PDR approximately equal to 88.7% by avoiding the busiest channels. This behavior was not observed during the simulations because we were in an ideal situation, the other channels did not present any other interference.

In case of attack, we observe that at the end of the simulation the PDR is around 60.5%, i.e. the detection threshold. Indeed, we have noticed after several experiments that the attacker has a significant effect after a few minutes, which is reflected by a significant drop in PDR from 81% to 58% at times 180 and 225. Then, the MAB-based channel hopping method changes its strategy because it receives steady 0 rewards for a certain time (the PDR being below the detection threshold). As the strategy changes, the attacker must adapt to

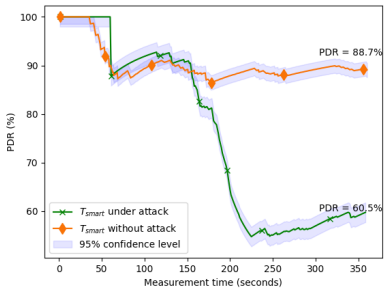

Fig. 5: PDR for smart channel hopping defense strategy against smart attacks

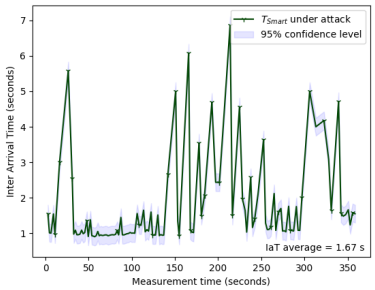

Fig. 6: IaT for smart channel hopping defense strategy against smart attacks

it. However, from second 250, the PDR remains close to the detection threshold. i.e. 60%.

The effectiveness of our attack is also confirmed by the total number of retransmissions showed in Tab. I. Although the total number of retransmissions generated by the attacker is smaller than when the victim uses basic channel hopping methods, our attack still causes a twofold increase. For the IaT metric, we observe in Fig. 6 that the MAB algorithm manages to limit the effects of jamming attacks. This method has higher performance than basic channel hopping strategies. Indeed, the IaT average for random channel hopping is equal to 2.16 seconds against 1.67 seconds for the smart strategy. Nevertheless, the attacker is able to delay transmissions (more than 2 seconds at a distance of 1 meter), therefore impacting the performance of the network. To conclude, we observe in Tab. II that our new jammer has a high accuracy even if the detection method is based on a smart approach. Indeed, after 5 minutes, the we achieve 62.5% attack accuracy.

IV. Discussion

The study and evaluation of different channel hopping strategies is crucial due to their use in many wireless protocols. Indeed, we find this logic of sharing the communication spectrum in several frequencies in certain addendum of the IEEE 802.11 protocol but also in 802.15.4 and Bluetooth. We show that channel hopping can be useful against interference generated by other legitimate networks. Indeed, numerous

wireless communication protocols communicate on the The 2.4 GHz Industrial, Scientific and Medical (ISM) band such as IEEE 802.15.4 and IEEE 802.11 protocols. In [12], authors implement a strategy based on channel hoping method to avoid interference between this two protocols. In addition to have interference between different wireless protocol, in a real-scenario like a building we can have interference generated with the same communication protocol.

The experimentation compared to the simulations made it possible to prove certain points. First, they made it possible to prove that this type of attack can be effective in real life and that integrating machine learning processes into attacks, represents a real danger. However, it was also able to show the effectiveness of different channel hopping methods under different scenarios. Although the smart channel hopping is considered to be a more innovative and effective method when an attack is present, we show here that in a scenario without an attack it is less effective than a basic method. In [5], the authors evaluated this technique in a fixed environment, i.e each channel had a fixed occupancy and interference rate throughout the experiment. In real situation, these parameters are variable and play a great role in the convergence time of the MAB algorithm. This is why, without attack this type of algorithm has more consequence on PDR than basic channel hopping method. In the event of an attack, this technique is more effective because it is less predictable at first by an attacker. Another important point that the experiments revealed is that this type of attack is possible in reality without requiring expensive hardware. In addition, the attacker does not need any prior knowledge except to know the communication protocol used by the victim. We have proven the effectiveness of this attack against several victim strategies and we have shown that the attacker can easily converge to the new channel used by the victim. Indeed, the number of retransmissions generated is 10 times greater than when no attack is present on the network. Finally, we would like to underline the dangerousness of this type of attack. In recent years, commercial drones developed by several companies such as DJI drones or the military drone have used this method of defense [13]. Testing this attack on this type of drone to disable it could be useful in defense strategies against drones flying over illicit areas. In this context, the channel hopping vulnerabilities highlighted in this paper could be an exploitable flaw for adversary to disable a drone.

One of possible countermeasures could be to deceive the smart attacker. Indeed as the attacker used a behavior analysis to elaborate their attack, the main idea could be to implement behavior variations on the victim's side. For example by providing false information (e.g false RSSI) or by making the decision to communicate on a wrong channel for a certain time. The goal would be for the attacker to converge on choosing an unused channel.

V. Conclusion

In this paper, we tested a novel MAB-based jamming attack. Through experimentation on a real testbed, we were able to evaluate different frequency hopping methods, from the simplest strategies to a more advanced strategy based on MAB. The results obtained show that frequency hopping can be useful in mitigating irregular interference from other APs that do not have the primary objective of creating attacks. In other words, splitting in the form of frequency is effective in allowing multiple networks to communicate on the same frequencies. On the other hand, frequency hopping seems to be ineffective against a smart jamming attack. Indeed when the access point uses a smarter frequency hopping system, the PDR drops from 88.7% to 60.5% on average against the same attack under the same time. Our work thus engages a possible opening on the use of these attacks against other systems using this mitigation. In future works, we will test this attack against a drone using the frequency hopping mitigation method and develop possible countermeasures.

References

[1] O. Bamahdi and S. Zummo, "An adaptive frequency hopping techniquewith application to bluetooth-wlan coexistence," in *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, 2006, pp. 131–131.

[2] M. Rahmanil, "Frequency hopping in cognitive radio networks: A survey," in *2015 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, 2015, pp. 1–6.

[3] H. Shin, K. Choi, Y. Park, J. Choi, and Y. Kim, "Security analysis of fhss-type drone controller." Berlin, Heidelberg: Springer-Verlag, 2015.

[4] H. Dakdouk, E. Tarazona, R. Alami, R. Féraud, G. Z. Papadopoulos, and P. Maillé, "Reinforcement learning techniques for optimized channel hopping in ieee 802.15.4-tsch networks," ser. MSWIM '18. New York, NY, USA: Association for Computing Machinery, 2018.

[5] V. Toldov, L. Clavier, V. Loscrí, and N. Mitton, "A thompson sampling approach to channel exploration-exploitation problem in multihop cognitive radio networks," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1–6.

[6] Y. Wang, Y. Niu, J. Chen, F. Fang, and C. Han, "Q-learning based adaptive frequency hopping strategy under probabilistic jamming," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2019, pp. 1–7.

[7] R. Gan, Y. Xiao, J. Shao, and H. Zhang, "Optimal attack strategy against wireless networked control systems with proactive channel hopping," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2436–2446, 2020.

[8] X. Cheng, J. Shi, M. Sha, and L. Guo, "Launching smart selective jamming attacks in wirelesshart networks," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, 2021, pp. 1–10.

[9] H. Noori and S. S. Vilni, "Jamming and anti-jamming in interference channels: a stochastic game approach," *IET Commun.*, vol. 14, pp. 682–692, 2020.

[10] E. Bout, A. Brighente, M. Conti, and V. Loscri, "Folpetti: A novel multi-armed bandit smart attack for wireless networks," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–10.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 46–57.

[12] J. Umer, H. Di, L. Peilin, and Y. Yueming, "Frequency hopping in ieee 802.15.4 to mitigate ieee 802.11 interference and fading," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 445–455, 2018.

[13] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progress in Aerospace Sciences*, vol. 91, 05 2017.