2021 36th Youth Academic Annual Conference of Chinese Association of Automation (YAC) | 978-1-6654-3712-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/YAC53711.2021.9486567

An Improved Frequency Hopping Algorithm Based on Transmission Scheduling against Jamming Attacks

Chenyuan Wang*, Xiangying Kong‡, Xuebing Chen†‡, and Xianghui Cao*†, *Senior Member, IEEE*

Abstract—**In wireless networked systems, jamming attacks are destructive and easy to be launched. To mitigate the jamming attack impact, frequency hopping is an effective way, in which a defender side can switch channels to avoid using the ones under jamming attack. However, the resilient ability of anti-jamming of traditional frequency hopping algorithm can't meet the requirement of communication without channel strategy and jamming detection under the circumstance of various forms of jamming attacks. In this paper, an improved frequency hopping algorithm with higher transmit success rate (TSR) has been proposed based on channel selection and adjustment of transmission time to defend different kinds of attacks such as reactive jamming, static jamming and scanning jamming. Our algorithm judges whether to adjust data transmission time according to the result of transmit success rate and use channel selection strategy to avoid most of interfered channels. Finally, our proposed algorithm is evaluated as a resilient scheme under different forms of jamming attacks through simulations.**

Index Terms—**Frequency hopping, Anti-jamming, Transmission scheduling, Channel selection**

I. Introduction

With the rapid development of Cyber-Physical Systems and Internet-of-Things paradigm, the request of better communication quality is becoming more frequent while establishing the network. However, nodes in a wireless network are vulnerable if there is no action to protect the security of data transmission [1]–[4].Jamming attack for communication network can be divided into passive attacks, active attacks and scanning jamming. How to build a reliable and safe scheme to guarantee data transmission between nodes is crucial in communication network [5]–[8].

The main reason why nodes are vulnerable to attack is that wireless devices transmit data on open frequency band in the communication between nodes. Active attack like reactive jamming detects the channel that devices transmit and actively broadcast interference signals. Other attack ways, such as static jamming, disrupt multiple channels in the open frequency band are effective due to the limit of channel numbers. To deal with these problems, traditional anti-interference approaches, including Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are mentioned. Compared to DSSS, FHSS technique is more resilient to interference signal and difficult to be conquered because data transmission process is divided into a large amount of time slots, in each slot sender and receiver select the random channel by its hopsets (the sequence of legal channel number) in a random time. However, FHSS will spend lots of time making sender and receiver hop into the same channel, which may cause unnecessary cost.

To the best of our knowledge, frequency hopping algorithms have been proposed to defend the interference attack [9]–[11]. Dynamic Adaptive Frequency Hopping (DAFH) algorithm is proposed to select more safe and admissible hopsets instead of full hopsets, the algorithms divide hopsets into many sub-hopsets and evaluate the channel level, sender will hop according to the result of channel security level [9]. In [10], the author proposes not only a low cost hopping algorithms, but also define maximal time rendezvous to guarantee the hopping time to transmit. The contribution of [11] considers the situation that channel interfered by heterogeneous attack and proposes rendezvous algorithm to guarantee best rendezvous performance.

In this paper, frequency hopping algorithm based on channel evaluation and dynamic transmission time adjustment has been proposed to avoid different kinds of interference. Our algorithm have better performance of data transmission on static jamming, reactive jamming and scanning jamming. In contrast to traditional frequency hopping, our algorithm can select the better channel and reduce time overhead in hopping. At the same time, time of data transmit will be dynamic adjusted in order to defend the detected interference signal.

The rest of this paper is organized as follows. Section II establishes the communication node model and introduces uncoordinated frequency hopping algorithm. Section III proposes our algorithm to defend different forms of jamming. Simulation and the result of algorithm comparison is shown in Section IV.

II. PRELIMINARIES

A. Communication Model

We first consider nodes in the wireless network communicate with each other using Wi-Fi 2.4GHz wireless bands, the division of the number of channels should take the influence of mutual interference into account. Besides, the number of hopping channel is consistent with open wireless spectrum in this paper. Besides, each node in wireless network has the

*School of Automation,Southeast University,Nanjing, China. Key Laboratory of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Nanjing, 210096, P. R. China Emails: {220191650,xhcao}@seu.edu.cn

†School of Cyber Science and Engineering, Southeast University, Nanjing, China Emails:99091cxb@163.com

‡Jiangsu Automation Research Institute, Lianyungang, Jiangsu, China

function of sending and receiving data on a certain channel. Considering the use of frequency hopping technology, all transmission time is divided into time slots and transmitter and receiver will select a new channel randomly when every time slot is over in order to avoid jamming.

We define channel sequences determine the channel set that nodes hop and the time of transmission. For example, assuming that hopsets of transmitter and receiver can be represented as H_{tx} = ($h_{1,tx}$, $h_{2,tx}$,...,$h_{n,tx}$) and H_{rx} = ($h_{1,rx}$, $h_{2,rx}$,...,$h_{n,rx}$), where $h_{i,tx}$, $h_{i,rx}$ $\in$ [0, N - 1] represents that transmitter and receiver visit the channel sequence between total N channel in ith slot of time slot and n represents the total time slot. Every node in network executes its sequences in a loop and the hop result in jth slot can be represented as $u^j = h_j \mod N$, transmitter and receiver will communicate successfully when they hop at the same frequency, i.e., $u_{j,tx}$ = $u_{j,rx}$.

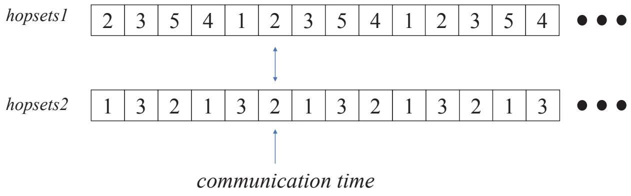

Fig. 1. Traditional uncoordinated frequency hopping algorithm

B. Jamming Model

The purpose of jamming attacker is to interference communication between nodes and cause the failure of most of the data packet transmission [12]. Jamming attacker usually interference all nodes within its jamming range r. According to different forms of jamming, attackers can be divided into static jamming and reactive jamming.

- Static jamming: Static jamming means that this kind of attack is unaware of the anti-jamming strategy of nodes. Static jammer attacks multiple channels in frequency bands constantly and thus data packets are easy to be dropped during transmission because most of channels are wasted. Assuming there is N channel numbers in open frequency bands and Static jammer will attack M channel in the long term.
- Reactive jamming: Reactive jammer will find the channel selected by transmitter firstly (supposing it is channel a) and then interference specific channel according to information of channel a [13].
- Scanning jamming: Scanning jamming means that attacker uses its jamming strategy to interference communications. If jamming strategy is unchanged, the possibility of successful jamming will not be high because of the flexibility of node defense strategy. On the other hand, jammer may learn from the law of defense strategy and adjust its strategy, which is more effective.

C. Traditional Uncoordinated Frequency Hopping Algorithm

The traditional uncoordinated frequency hopping (UFH) algorithm has been considered as an effective way to defend jamming attack, due to randomly channel selection and uncoordinated data transmission (see Fig.1). Uncoordinated data transmission means that transmitter and receiver use hopsets to choose a randomly channel at any time in the time slot instead of transmitting the share message that contains the information of selecting channel [14]. it is obvious that traditional uncoordinated frequency hopping algorithm can defend interference attack and improve the ability of jamming resilient.

However, considering different forms of jamming attack, uncoordinated frequency hopping may face many challenges in data transmission,which will reduce the reliability of communication (see Fig.2). Due to the ignorance of considering jamming detection, uncoordinated frequency hopping has a great probability of selecting a contaminated channel for communication under the situation that multiple channels are interfered. Moreover, uncoordinated frequency hopping can't prevent attacker from detecting the channel that nodes communicate, thus reactive jamming will work as long as the total time from detection channel to the arrival of the interference signal at the communication node is less than the time of data transmission slot.

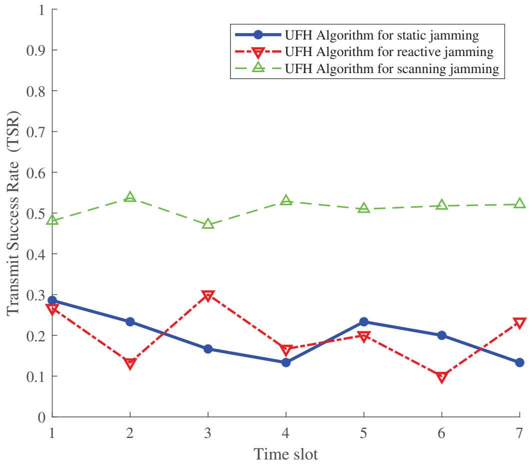

Fig. 2. Uncoordinated frequency hopping algorithm for jamming

III. The Proposed Algorithm

In this section, we present a frequency hopping algorithm based on the channel selected and dynamic transmission adjustment in order to guarantee the resilient ability of wireless network against different forms of jamming attack. As illustrated in Algorithm 1, the steps for proposed frequency hopping algorithm are as follows, the procedure of the proposed algorithm is express as Fig.3:

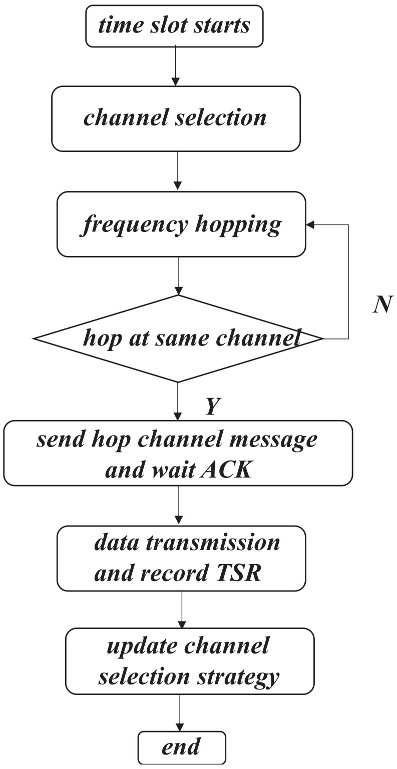
time slot starts
channel selection
frequency hopping
hop at same channel
N
Y
send hop channel message and wait ACK
data transmission and record TSR
update channel selection strategy
end

Fig. 3. The procedure of the proposed algorithm

A. Channel selection and frequency hopping

When time slot begins, transmitter detects the frequency bands and finds the channel that is not to be wasted by using jamming detection as a prior knowledge. It is worthy that using jamming detection as a prior knowledge is not absolutely accurate and the status of frequency bands will change after channel detection, so other strategy should be considered to improve the success rate of transmission. Moreover, every node defines channel weight array $W = \{\omega_1, \omega_2, ..., \omega_N\}$ to determine which channel nodes transmit and the length of array is N. Jamming detection will evaluate the status of the channel by SNR model and update channel weight array. The channel C_i^j that node i chooses in j slot can be expressed as:

$$c_i^j = max\left\{\omega_1, \omega_2, ..., \omega_N\right\} \tag{1}$$

Then, the result will be encapsulated in a secret message and sent to receiver using traditional uncoordinated frequency hopping. Besides, the transmitter waits for an ACK packet that sender replies. we use Maximum Time-To-Rendezvous (MTTR) and $t_{transmit}$ to calculate to time that ACK message arrives because MTTR means that hopsets coincide within MTTR time and $t_{transmit}$ represents the time that ACK and secret message transmit. $t_{transmit}$ and MTTR metric can be express as:

$$MTTR = t_{rend} - t_{start} \tag{2}$$

$$t_{rend} = \{\ t \mid \text{when } u_{trans} = u_{rec}\ \} \tag{3}$$

$$t_{transmit} = 2 * D/c \tag{4}$$

Where t_{start} is the time when time slot starts in $Eq.2$, t_{rend} represents the time from time slot starts to rendezvous and the definition of rendezvous has shown in Section II. In $Eq.3$, D represents the distance between transmitter and receiver and c is speed of light. After the following procedure is over, the process of data transmission will start.

B. Data transmission

In the process of data transmission, transmitter sends data packets at a certain rate and receiver replies ACK packet when a data packet arrives. The count of data packets N_{sum} and ACK packets N_{suc} will be recorded when the current time slot is over.

When data transmission of each time slot is over, the success rate of data transmission in this process will be used to measure the quality of data transmission. Define TSR as the success rate of data transmission and we use it to update channel weight array W. The transmission between transmitter and receiver on a non-jamming channel if TSR is close to 1. On the contrary, if TSR is lower than a threshold, it means that jamming attack has interference the selected channel, the weight of this channel in channel weight array will be updated and the probability of selected channel will decrease in the future time slot. The formula that using exponential moving average for channel update is as follows:

$$TSR = N_{suc}/N_{sum} \tag{5}$$

$$\omega_{new}^i = \gamma\omega_{old}^i + (1-\gamma)TSR \tag{6}$$

In the above equation, i represents in the current time slot and nodes communicate on channel i. TSR will be a relatively low value when the data transmission channel is interferenced and affect ω_{new} become lower. γ is weighing factor to decide whether nodes pay more attention to actual transmission situation because TSR is based on data transmission statistics in the current time slot. Considering that there are different types of jamming by attackers and historical channel weights ω_{old}^i is only effective in static attacks, γ should be set to a small value to improve the performance of reactive jamming. Due to the tendency of selecting higher weight channel, the scheme will exclude channel with poor communication quality. Besides, when interference is detected, the time of data transmission will be shortened in the future slot to prevent reactive jamming. Fig.4 and Fig.5 show the procedure of above steps from the perspective of time.

Algorithm 1 shows the above process of the proposed algorithm: N represents the channel numbers and correspond to channel weight vector $\omega = [\omega^1, \omega^2, ..., \omega^N]$ (where ω^i means weight of each channel). Moreover, hop result of node u_{node} decides when they transmit and data transmission time T_{tran} is the time of data transmission, $t_{datatrans}$ represents the time that one data packet transmits. Eventually, transmission threshold T_h and adjustment factor δ_{adjust} have been considered as the input of the proposed algorithm.

Algorithm 1 Procedure of the proposed algorithm based on adjustment of transmission time

```
Input: $N$, $\omega$, $u_{node}$, $T_{tran}$, $T_h$, $\delta_{adjust}$ , $t_{datatrans}$ and $t \leftarrow 0$
Output: $TSR$
Initialize the $N$, $W$ ;
Select the best channel c according to channel weight matrix $c \leftarrow max\{\omega_1, \omega_2, ..., \omega_N\}$;
while $u_{tx}$ != $u_{rx}$ do
    $u_{tx} \leftarrow h_j \mod N$;
    $u_{rx} \leftarrow h_j \mod N$;
end while
send secret message and receive ACK;
Data transmission period starts:
while $t <= T_{tran}$ do
    Transmitter sends data packet;
    $N_{sum} \leftarrow N_{sum} + 1$;
    if ACK packet arrives then
        $N_{suc} \leftarrow N_{suc} + 1$;
    end if
    $t \leftarrow t + t_{datatrans}$;
end while
$TSR \leftarrow N_{suc}/N_{sum}$;
$\omega^i_{new} \leftarrow \gamma\omega^i_{old} + (1 - \gamma)TSR$;
if $TSR < T_h$ then
    $T_{tran} \leftarrow T_{tran} * \delta_{adjust}$
end if
Next time slot starts ;
```

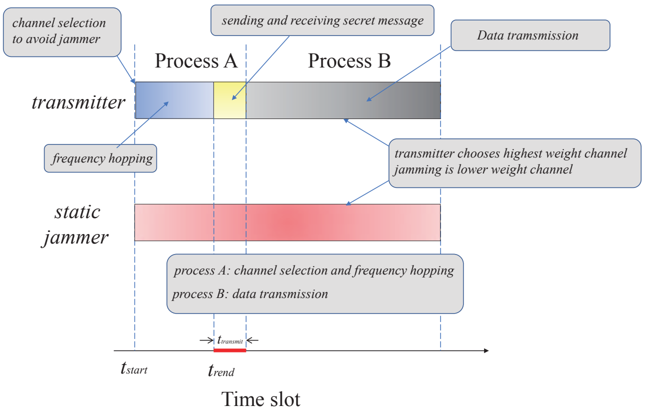
channel selection to avoid jammer
sending and receiving secret message
Data tramsmission
Process A
Process B
transmitter
frequency hopping
transmitter chooses highest weight channel jamming is lower weight channel
static jammer
process A: channel selection and frequency hopping
process B: data transmission
$t_{transmit}$
t_{start}
t_{rend}
Time slot

Fig. 4. The example of proposed frequency hopping algorithm

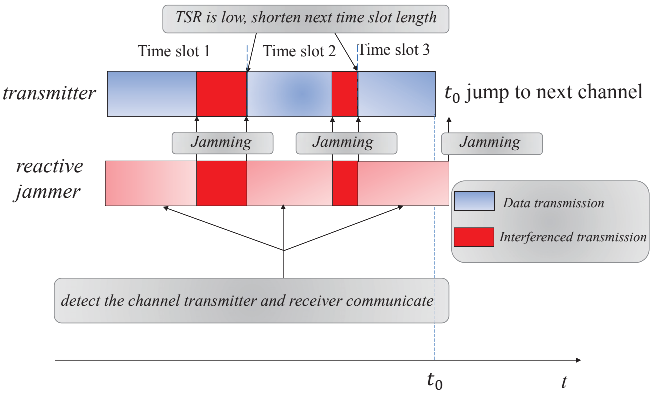
TSR is low, shorten next time slot length
Time slot 1
Time slot 2
Time slot 3
transmitter
t_0 jump to next channel
Jamming
Jamming
Jamming
reactive jammer
Data transmission
Interferenced transmission
detect the channel transmitter and receiver communicate
t_0
t

Fig. 5. The example of time scheduling algorithm

C. Effectiveness of our proposed algorithm

1) Static jamming: In contrast to uncoordinated frequency hopping, the proposed algorithm generates a secret message that contains the information of selected channel in the current time slot. To prevent jammer from secret message interference, uncoordinated frequency hopping is used to send secret message to the receiver, it ensures that each slot secret message is sent in a random channel and moment, which guarantees the success transmission of the secret message. Due to existence of channel evaluation, communication nodes can distinguish the clean channel even if multiple jamming interferes with most channel. Static jamming don't care node defense strategy and interference most of channels, so proposed algorithm will defend static jamming because non-jamming channel has been distinguished according to channel weight matrix.

2) Reactive jamming: Considering of reactive jamming, as is shown in Fig.5, the time of data transmission will dynamically adjust and eventually shorter than the total time from jamming detection to interference signal comes. The key of defensing reactive jamming is that time of entire process should faster than the frequency of interference. Dynamic time adjustment continuously shortens the time of the entire transmission process to ensure the security of the process of data transmission.

3) Scanning jamming: The threat of scanning attacks is that jammer may find the rule of defense strategy and improve the success rate of jamming. Considering of our situation, it means that TSR will be cracked and jammer knows that node chooses channel based on TSR at the same time. Eventually, jammer establishes its channel weight channel and choose the highest weight channel to interference. However, according to $Eq.6$, channel weight ω_{new} determined by not only TSR but also history weight ω_{old}, and it is obvious that γ in equation is unknown to attacker because node will not send it to anyone. Moreover, jammer can't infer when data transmission starts and ends, it causes that the TSR of jammer and node is not same. Based on above aspects, jammer can not find the correct weight channel and thus can't interference data transmission.

D. Discussion of intelligent form of jamming

In this section, we discuss a intelligent form of jamming that jammer knows the defense strategy of wireless node, it means that jammer knows that the basis for the node to choose channel communication is the success rate of data transmission in each time slot. Then, jammer will establish its own channel selection strategy to jam the highest weight channel. This kind of jamming will take effect as well as the following conditions meet: the information of TSR of all time slot are known by jammer and jammer can evaluate the selection weight of all channels accurately.

It is difficult to meet the above conditions at the same time. Firstly, the information of TSR are hard to be detected by jammer. In the scenario that our paper proposes, TSR is correspond to the number of packets that are sent and received successfully, and jammer can not detect which packet is successfully send because node that under jamming has a low possibility of sending packet, assuming it is p, the TSR that jammer evaluates TSR_j and node counts TSR_n can be express as follows:

$$TSR_j = N_{no-jam}/N_{sum} \tag{7}$$

$$TSR_n = N_{no-jam} + p * N_{jam}/N_{sum} \tag{8}$$

In the above equations, N_{no-jam} and N_{jam} represent the success transmission number of packets under non-jamming and jamming data transmission time and N_{sum} represents the sum of packets in one time slot. It is obvious that the TSR that jammer evaluates TSR_j and node counts TSR_n are not the same, it means that intelligent form of jammer can't evaluate the channel selection strategy of wireless node and thus jamming will take no effect.

IV. SIMULATION

In this section, we use OMNeT++ to simulate UFH algorithm and the proposed algorithm to analyze the performances of data transmission under different forms of jamming attacks. In UFH, each node uses hopsets to jump to a random channel in every time slot and is vulnerable to jamming. In the following simulation, different forms of attackers are applied to interfere wireless nodes, including reactive jammers and multiple channel jammers. Reactive jammers detect the communication channel firstly and interfere it with same frequency after a period of time(related to signal transmission). Multiple channel jammers attack multiple channel in a limited number of channels. Transmit success rate (TSR), the ratio of the number of successfully transmitted data packets to the total data packets, is regarded as the metric that evaluates UFH algorithm and the proposed algorithm.

In OMNeT++ simulation environment Qtenv, transmitter and receiver pair communicate with each other and jammer interferes all nodes within communication range r, if transmitter sends a data packet and does not receive the corresponding ACK packet, it means that this data packet is jammed and fail to transmit. In order to eliminate the influence of mutual interference as much as possible, the channel number N is set to 11 refers to Wi-Fi 2.4GHz open frequency bands. At the end of time slot, transmit success rate will be recorded. Besides, if nodes communicate on uncontaminated channel, transmit success rate of data is set to 80% and 20% in interfered channel to make data transmission more realistic.

In the OMNeT++ simulation, it is obvious that our algorithm with channel select and time adjustment has better transmit success rate whatever reactive jamming, scanning or multiple jamming referred to Fig.6, Fig.9 and Fig.10, this is because that proposed usually find the best channel to communicate, which prevents multiple channel jamming. Even if reacting jamming will interfere successfully in very few moments due to the awareness of data transmission time, our algorithm will dynamic adjust the period of transmission and thus reactive jamming become invalid because entire time slot will shorten compared to jamming frequency in next few time slots. Besides, we set different ω to test the performance of the proposed algorithm. If this metric is close to 1, it means that TSR will have a large weight in channel selection in $Eq.6$.

It is worth noting from Fig.6 that the result of UFH algorithm under the attack of static jamming for the first time slot is higher than other slots, which means that UFH algorithm avoids interference in this slot. This is because uncoordinated frequency hopping selects randomly channel in each time slot and it has fewer probability that an uncontaminated channel can be selected. The same circumstance will not happen under reactive jamming because reactive jammer always gets the status of all channels before sending interference noise.

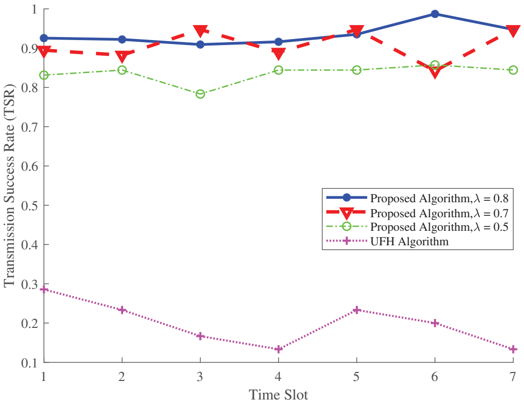

Fig. 6. TSR performance of different algorithm under static jamming

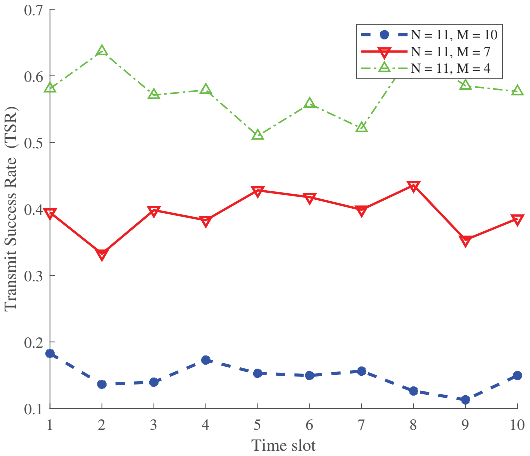

Fig. 7. TSR performance of UFH algorithm under different number of interference channels

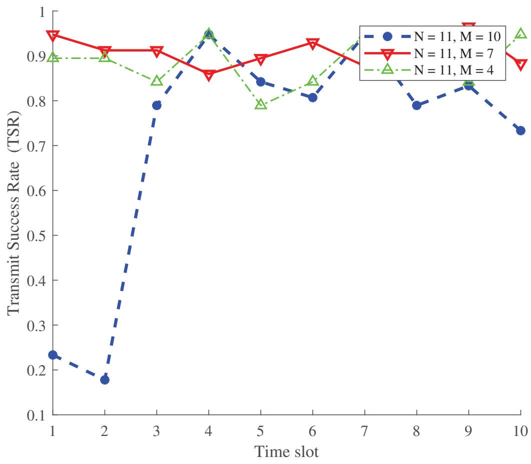

Fig. 8. TSR performance of the proposed algorithm under different number of interference channels

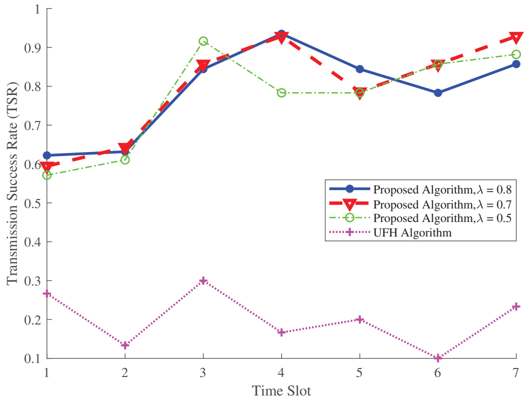

Fig. 9. TSR performance of different algorithm under reactive jamming

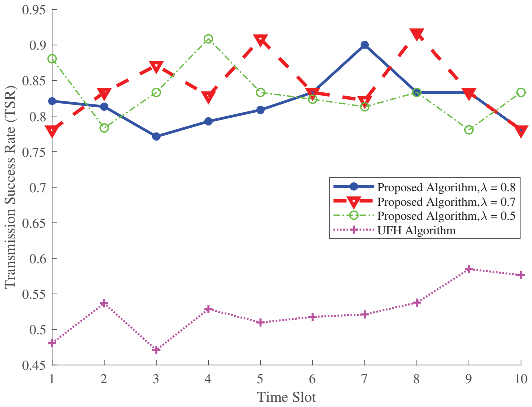

Fig. 10. TSR performance of different algorithm under scanning jamming

V. CONCLUSION

Recalling that UFH algorithm is hard to defend different forms of jamming without the scheme of jamming detection and transmission adjustment. In this paper, we propose an algorithm based on channel evaluation and time adjustment strategy. According to OMNET simulation, proposed algorithm has higher transmit success rate under different forms of jamming attacks.

VI. ACKNOWLEDGEMENT

This work was supported by the National Natural Science Foundation of China under Grant 92067111, the Outstanding Young Scholarship of Jiangsu Province under Grant BK20180012, and the Zhongying Young Scholars Project.

REFERENCES

[1] Y. Zhu and W. X. Zheng, “Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy,” *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3714–3721, 2019.

[2] J. Yao, R. Jiang, and W. Heng, “Algebraic construction of optimal frequency hopping patterns based on welch costas arrays,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1841–1854, 2019.

[3] Q. Wang, H.-N. Dai, H. Wang, G. Xu, and A. K. Sangaiah, “Uav-enabled friendly jamming scheme to secure industrial internet of things,” *Journal of Communications and Networks*, vol. 21, no. 5, pp. 481–490, 2019.

[4] J. Heo, J.-J. Kim, J. Paek, and S. Bahk, “Mitigating stealthy jamming attacks in low-power and lossy wireless networks,” *Journal of Communications and Networks*, vol. 20, no. 2, pp. 219–230, 2018.

[5] F. J. Escribano, A. Wagemakers, G. Kaddoum, and J. V. Evangelista, “A spatial time-frequency hopping index modulated scheme in turbulence-free optical wireless communication channels,” *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4437–4450, 2020.

[6] L. Zhu, M. Farhat, Y.-C. Chen, K. N. Salama, and P.-Y. Chen, “A compact, passive frequency-hopping harmonic sensor based on a microfluidic reconfigurable dual-band antenna,” *IEEE Sensors Journal*, vol. 20, no. 21, pp. 12495–12503, 2020.

[7] K. Wu, J. A. Zhang, X. Huang, Y. J. Guo, and R. W. Heath, “Waveform design and accurate channel estimation for frequency-hopping mimo radar-based communications,” *IEEE Transactions on Communications*, 2020.

[8] C. Han, A. Liu, H. Wang, L. Huo, and X. Liang, “Dynamic anti-jamming coalition for satellite-enabled army iot: A distributed game approach,” *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10932–10944, 2020.

[9] P. Popovski, H. Yomo, and R. Prasad, “Strategies for adaptive frequency hopping in the unlicensed bands,” *IEEE Wireless Communications*, vol. 13, no. 6, pp. 60–67, 2006.

[10] G.-Y. Chang, J.-F. Huang, and Z.-H. Wu, “A frequency hopping algorithm against jamming attacks under asynchronous environments,” in *2014 IEEE Global Communications Conference*, pp. 324–329, IEEE, 2014.

[11] Z. Gu, T. Shen, Y. Wang, and F. C. Lau, “Efficient rendezvous for heterogeneous interference in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 91–105, 2019.

[12] Q. Sun, T. Shu, K.-B. Yu, and W. Yu, “Efficient deceptive jamming method of static and moving targets against sar,” *IEEE Sensors Journal*, vol. 18, no. 9, pp. 3610–3618, 2018.

[13] S. Sciancalepore, G. Oligeri, and R. Di Pietro, “Strength of crowd (soc)—defeating a reactive jammer in iot with decoy messages,” *Sensors*, vol. 18, no. 10, p. 3492, 2018.

[14] J. S. Sousa and J. P. Vilela, “Uncoordinated frequency hopping for wireless secrecy against non-degraded eavesdroppers,” *IEEE transactions on information forensics and security*, vol. 13, no. 1, pp. 143–155, 2017.