Liu *et al. J Wireless Com Network* (2021) 2021:152
https://doi.org/10.1186/s13638-021-02029-8

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Novel channel-hopping pattern-based wireless IoT networks in smart cities for reducing multi-access interference and jamming attacks

Yiming Liu[1,2], Qi Zeng[3], Yue Zhao[1,2*], Kaijun Wu[1,2] and Yao Hao[1,2]

*Correspondence: yuezhao@foxmail.com
[1] Science and Technology on Communication Security Laboratory, Chengdu, China
Full list of author information is available at the end of the article

Abstract

In smart cities, the Internet-of-Thing (IoT) provides an enabling communication infrastructure to support tremendous amount of data exchange. Most IoT applications, e.g., wireless local area network, Bluetooth and so forth, utilize the channel-hopping scheme to suppress the transmission security threats. In this paper, to reduce the mutual interference and external jamming attacks, multiple novel channel-hopping patterns, i.e., traditional no-hit-zone (NHZ) hopping pattern and generalized NHZ hopping pattern, are introduced to suit to IoT networks. Particularly the design of probabilistic hopping pattern is first proposed, which has the various usage probabilities with regard to various channels. The properties of these hopping patterns are investigated by the step-to-step examples. Then, the error-rate performance of the multi-node IoT systems adopting these hopping patterns in the presence of jamming attacks is comprehensively analyzed. The extensive simulations show that the traditional/generalized NHZ hopping patterns are in favor of combating the mutual interference but with the limited capability of reducing jamming attacks, while the probabilistic hopping pattern possesses the opposite feature, that is, it has the predominant merit in suppressing jamming attacks. Thus, the novel channel-hopping pattern-based IoT could provide the secure transmission for communication applications in smart cities. Note that, as the physical-layer security technique, the channel-hopping patterns investigated in this paper are convenient to integrate with the security policies implemented in upper layers (e.g., encryption, authentication and so forth).

Keywords: Wireless IoT networks, Jamming attacks, Interference, Design of channel-hopping patterns, System analysis

1 Introduction

The smart cities contain lots of applications and sensors nodes, such as smart home appliances, smart grid applications, weather and temperature sensors, smart buildings and so forth [1, 2]. Wireless Internet-of-Things (IoT) networks provide the ubiquitous infrastructure for connecting these massive sensor nodes [3]. The IoT networks are characterized by the open architecture allowing the legitimate nodes to conveniently access to each other; however, this architecture causes the severe cyber-security issues emitted by the vicious nodes, e.g., denial-of-service attacks, eavesdropping, privacy and jamming

attacks. The previous solutions to the cyber security mainly focused on encryption and authentication in the upper layers [4–10], but they are ineffective to the denial-of-service attacks (e.g., jamming and interference). Besides, most of wireless IoT applications, such as WiFi, Zigbee, RFID, Bluetooth and forth, operate simultaneously in the unlicensed industrial–scientific–medical (ISM) band [3, 11–13]. The legitimate nodes (users) in these applications communicate to the corresponding destinations by sharing the limited spectrum, which lead to the mutual interference when the nodes occupy the same channel. Thus in the physical and media access layers, the mutual interference and the hostile jamming attack are the main impacts on the performance of wireless IoT, which have attracted lots of attentions in industry and academics [14–19]. The physical-layer security techniques offer distinct advantages compared to cryptography and authentication, because these techniques have high scalability but are independent on computational complexity.

To deal with the aforementioned issues, the channel-hopping scheme is one of the most efficient solutions in the multi-node (i.e., multiple legitimate users) IoT networks in the presence of jamming attacks [20–26]. Since the jammer emits the threat of malicious signal by randomly scanning the channels, the legitimate nodes can avoid such a threat by quickly changing the active channels. Also, for the multiple legitimate users, minimizing amount of mutual channel hits of the employed channel-hopping pattern can efficiently suppress the mutual interference. The channel-hopping scheme can be implemented, respectively, by the frequency-hopping (FH) or the time-hopping (TH) techniques in the spectral domain or time domain. It is noted that the properties of channel-hopping pattern determine the capacity of anti-interference and anti-jamming. These critical properties include Hamming correlations and uniformity [27]. The Hamming correlations describe the number of the channel hits, which imply the level of mutual- and self-interferences. The uniformity denotes how random the hopping rule of channels is, which is related to the capacity of anti-jamming attacks and anti-eavesdropping threats. Thus, the design of channel-hopping pattern with favorable Hamming correlations and uniformity is the critical challenge in multi-node IoT communications.

Up to now, the design of channel-hopping patterns including FH/TH patterns (sequences) has been one of hot research topics in the region of information theory [28–31]. To achieve the optimal design of multi-node FH/TH access systems, the optimal trade-offs with regard to the hopping pattern parameters (e.g., the size of available channels q, the length of hopping pattern L, the number of hopping patterns K, the Hamming correlations of hopping pattern $H_{c,a}$, etc.) have been established, such as Lempel–Greenberger bound [32], Peng–Fan bound [33] and Ye–Fan bound [34]. Most *optimal* channel-hopping patterns [28–30, 33] have been designed to meet the aforementioned bounds. For example, a series of design algorithms for traditional pseudo-random hopping patterns has been developed using various algebraic or combinational tools to hold Peng–Fan bound (see [28–30]). The channel hits of these hopping patterns always follow the (almost) uniform distribution, which may cause a few amount of multiple-access interference (MAI) and consequently the performance degradation in multi-access systems. Recently, a novel hopping pattern, called no-hit-zone hopping pattern (NHZ), was proposed, which owns the orthogonality for small access delays around the origin [34–36]. In [37], a generalized NHZ hopping pattern which enjoys orthogonality for small

access delays as well as least channel hits otherwise. The traditional/generalized NHZ hopping patterns have the superior capability of mitigating the mutual interference, compared to the other pseudo-random hopping patterns.

Since some of transmitting channels may be attacked by the hostile jammers, the system performance could be degraded if the signals are transmitted on these impaired channels. All existing pseudo-random hopping patterns tread all channels having the same condition (i.e., following the uniformity), without considering the probability of jamming attack on these channels [28–30, 33–37]. In this paper, we propose a so-called probabilistic hopping pattern, where the usage probabilities of the channels are changed with the different channel qualities. That is, the channels with the lower probability of jamming attack are utilized with the high probability and vice versa. Under the constraint of the usage probabilities of the channels, minimizing the Hamming correlations of such a hopping pattern is another target of pattern design. This is the first contribution in this paper.

The second objective of this paper is to evaluate the error probability performance of a multi-node IoT system employing these hopping patterns in the presence of jamming attacks. For analysis convenience, the multi-node IoT system is modeled as FH multi-access system with the frequency-shift keying modulation (i.e., FSK/FHMA system) in this paper. We derive the analytic expressions of decision variable of the multi-node IoT system under a slow Rayleigh fading channel. The bit-error-rate (BER) performance of these investigated hopping patterns imposed in multi-node IoT systems is evaluated by simulations.

2 Methodology of analysis and experiment

The methodology and the organization of this paper are presented as follows. The definitions of traditional/generalized NHZ hopping patterns are recalled. The traditional/generalized NHZ hopping patterns, which have become the promising pseudo-random hopping patterns recently, are treated as the benchmark in this paper. Then, a novel channel-hopping pattern called probabilistic hopping pattern is constructed by using algebraic transformations and replacing algorithm based on prime hopping pattern. Subsequently, by setting the specific parameters, some examples of traditional/generalized NHZ hopping patterns and probabilistic hopping pattern are presented to verify their properties. The properties among these hopping patterns are clearly compared. Subsequently from the viewpoint of system performance, the signal analysis of the multi-node IoT system employing with the aforementioned channel-hopping patterns is conducted in the presence of jamming attacks. The signal processing is strictly conducted via the stochastic process methods. Based on the signal analysis, the BERs of multi-node IoT systems are investigated by Monte Carlo simulations. Finally, we draw some conclusions.

3 Pseudo-random channel-hopping patterns

In this section, we will introduce the definitions of several pseudo-random channel-hopping patterns (sequences), which have the various properties with each other. These channel-hopping patterns include traditional NHZ hopping pattern and generalized NHZ hopping pattern. Before presenting the definitions, some notations with regard to the hopping pattern are explained as follows,

- q: the number of the available channels;
- L: the length of the hopping pattern;
- K: the number of sequences in the channel pattern;
- $\mathbb{S}$: the channel-hopping pattern accommodating K legitimate users, which is denoted as $\mathbb{S} = \{\mathbf{S}^{(k)}, k = 1, 2, \ldots, K\}$.
- $\mathbf{S}^{(k)}$: the channel-hopping sequence for the kth legitimate user.

3.1 Hamming correlation of the channel-hopping pattern

Hamming correlation is one of the most critical property of FH pattern, i.e., the number of channel hits, will be presented as follows.

Definition 1 Given two channel-hopping sequence of length L,

$$\begin{aligned}\mathbf{S}^{(i)} &= \left(s_0^{(i)}, s_1^{(i)}, \ldots, s_{L-1}^{(i)}\right),\\ \mathbf{S}^{(j)} &= \left(s_0^{(j)}, s_1^{(j)}, \ldots, s_{L-1}^{(j)}\right),\end{aligned} \tag{1}$$

where $\mathbf{S}^{(i,j)}$ are selected from the channel-hopping pattern $\mathbb{S}$. The Hamming cross-correlation $H_c(\cdot)$ and Hamming auto-correlation $H_a(\cdot)$ at the delay τ are defined as, respectively

$$H_c\left(\tau|\mathbf{S}^{(i)}, \mathbf{S}^{(j)}\right) = \sum_{l=0}^{L-1} h\left[s_l^{(i)}, s_{l+\tau}^{(j)}\right],\ i \neq j, \tag{2}$$

$$H_a\left(\tau|\mathbf{S}^{(j)}\right) = \sum_{l=0}^{L-1} h\left[s_l^{(j)}, s_{l+\tau}^{(j)})\right], \tag{3}$$

where $h[x, y] = 1$ for $x = y$ representing the channel slot x colliding with another one y, whilst $h[x, y] = 0$ for $x \neq y$ representing the hit-free. The subscript addition $(\cdot)_{i+\tau}$ is performed modulo L.

The Hamming correlations are the important properties in IoT systems based on channel-hopping scheme, which determine the mutual- and self-channel hits, as well as the capacity of combating multi-path fading and so forth.

3.2 Traditional NHZ hopping pattern

Definition 2 Given a channel-hopping pattern $\mathbb{S} = \{\mathbf{S}^{(k)}, k = 1, 2, \ldots, K\}$ with K sequences, where $\mathbf{S}^{(k)} = \{s_l^{(k)}, l = 0, 1, \ldots, L-1\}$ is the hopping sequence for kth legitimate user and the element $s_l^{(k)}$ is generated over q available channels. $\mathbb{S}$ is called as *NHZ hopping pattern* with no-hit zone Z, when the Hamming auto- and cross-correlations ($H_a(\tau)$ and $H_c(\tau)$) satisfy, respectively

$$\begin{aligned} &H_a\left(\tau|\mathbf{S}^{(i)}\right) \equiv 0;\ \text{when } |\tau| \leq \mathrm{Z}, \forall \mathbf{S}^{(\mathrm{u})} \in \mathbb{S} \\ &H_c\left(\tau|\mathbf{S}^{(i)}, \mathbf{S}^{(j)}\right) \equiv 0;\ \text{when } 0 < |\tau| \leq \mathrm{Z}, \forall \mathbf{S}^{(\mathrm{u})}, \mathbf{S}^{(\mathrm{v})} \in \mathbb{S}, \mathrm{u} \neq \mathrm{v} \end{aligned} \tag{4}$$

The NHZ hopping pattern is usually denoted as $\mathbb{S}(q, L, K, Z)$ in previous studies. □

By the definition of NHZ hopping pattern, it is observed that the Hamming auto- and cross-correlations of NHZ hopping pattern are equal to zero if the delay τ is limited within Z. Such properties can guarantee the orthogonality for the multiple legitimate users accessing the network as long as the multiple users are strictly limited in the small access delay. However in the practice, particularly in the presence of jamming attacks, the small access delay is hard to realize due to the synchronization attack; consequently, the NHZ hopping pattern will cause the server performance degradation. The construction of traditional NHZ hopping patterns can be found in [35–37].

3.3 Generalized NHZ hopping pattern

Extending the definition of traditional NHZ hopping pattern, we further focus on the maximum Hamming cross- and auto-correlations of $\mathbb{S}$ when τ is outside of Z, i.e., $(Z_{nh} + 1 \leq |\tau| \leq L - 1)$, which are shown as

$$\begin{aligned} H_a &= \max\left\{H_a\left(\tau|\mathbf{S}^{(i)}\right)|\mathbf{S}^{(i)} \in \mathbb{S}, Z+1 \leq |\tau| \leq L-1\right\}, \\ H_c &= \max\left\{H_c\left(\tau|\mathbf{S}^{(i)}, \mathbf{S}^{(j)}\right)|\mathbf{S}^{(i)}, \mathbf{S}^{(j)} \in \mathbb{S}, i \neq j, Z+1 \leq |\tau| \leq L-1\right\}. \end{aligned}$$

The maximum Hamming correlation outside of Z is defined as

$$H_m = \max\{H_a, H_c\}. \tag{5}$$

A fundamental trade-off between $\{q, L, K, Z, H_m\}$ has been established in [37] as follows.

Theorem 1 *The lower bound of generalized NHZ hopping pattern is presented as following* [37]:

$$H_m \geq \frac{KL^2 - qL}{q\left\lfloor \frac{L}{Z+1} - 1 \right\rfloor + q(K-1)\left\lfloor \frac{L}{Z+1} \right\rfloor}. \tag{6}$$

Definition 3 A NHZ hopping pattern achieving the equality in (6) is called a generalized NHZ hopping pattern, which is denoted by $\mathbb{S}(q, L, K, Z, H_m)$ for simplicity [37].

By the above definition, the generalized NHZ hopping pattern satisfies the orthogonality for the small access delays $|\tau| \leq Z$, whilst having minimum amount of channel collisions for $|\tau| > Z$. Such properties imply that, even if, in the presence of the synchronization attacks, the performance degradation could be minimized. The generalized NHZ hopping patterns have the unique advantage compared to the other pseudo-random hopping patterns.

4 Probabilistic hopping pattern and construction algorithm

In the existing pseudo-random hopping patterns including the traditional/generalized NHZ hopping patterns, the change rule of channel follows the (nearly) uniform distribution over the available channels. These channel-hopping patterns cannot take account of the status of jamming attack and cannot learn about the channel state information in advance. The drawback of such hopping schemes is that the legitimate users hop from one channel to another according to the pre-assigned hopping pattern, no matter what probability of jamming attack is emitted or not.

In this paper, we firstly propose a novel probabilistic hopping pattern (Prob-HP), where the usage probabilities of the channels correspond to the occurrence probability of jamming attacks.

4.1 Definition of probabilistic hopping pattern

Definition 4 Given a channel-slot set $\mathbb{F} = \{f_0, f_1, \ldots, f_{q-1}\}$ and its channel quality measured by the index of channel-gain $\mathbb{H} = \{h_0, h_1, \ldots, h_{q-1}\}$, where h_i denotes the channel gain of the ith channel f_i. In $\mathbb{F}$, the channel slots are reordered by their qualities (i.e., the channel f_0 has the best quality, and f_{q-1} is the poorest one). We assume that p_i presents the probability of f_i appearing in the hopping pattern. The Prob-HP $\mathbb{S}$ with length of L and size of K is generated over $\mathbb{F}$ and should satisfy that

$$\begin{aligned} &p_0 \geq p_1 \geq p_2 \geq \cdots \geq p_{q-1}, \\ &\sum_{i=0}^{q} p_i = 1. \end{aligned} \tag{7}$$

where the values of $\{p_i | i = 0, 1, 2, \ldots, p-1\}$ are determined by the corresponding channel gains, that is, $p_i = \frac{\mathbb{E}\{|h_i|\}}{\sum_i \mathbb{E}\{|h_i|\}}$, where $\mathbb{E}\{\cdot\}$ denotes the expectation operator. The optimal Prob-HP $\mathbb{S}$ should satisfy that the Hamming correlations $H_a(\cdot)$ and $H_c(\cdot)$ are as small as possible.

In particular when the equality is (approximately) hold in (7), it is simplified to be the traditional uniformly distributed hopping pattern. The probability of each channel in the traditional pseudo-random pattern p_i is (approximately) equal to $1/q$.

4.2 Construction algorithm of Prob-HP

A construction algorithm of Prob-HP consists of two steps, which will be presented as follows.

Step 1 Constructing a prime hopping pattern $\mathbb{P}$ over the given a channel-slot set $\mathbb{F} = \{f_0, f_1, \ldots, f_{q-1}\}$ with a prime value q [27]. A new hopping pattern $\mathbb{Q}$ is formed by the cascade operation of m items of $\mathbb{P}$, i.e., $\mathbb{Q} = [\mathbb{P}, \mathbb{P}, \ldots, \mathbb{P}]$. The value of m is determined by the intend probability of each channel $\{p_i\}_i$. The $\mathbb{Q}$ can be rewritten row by row as follows:

$$\mathbb{Q} = \{\mathbf{Q}_0, \mathbf{Q}_1, \ldots, \mathbf{Q}_{q-1}\}. \tag{8}$$

It is easy to obtain that the probability of each channel appearing in each sequence $\mathbf{Q}_k$ is $\bar{p} = 1/q$ according to the properties of prime hopping pattern.

Step 2 Assuming that the channel gains of $\mathbb{F}$ are the prior knowledge to the legitimate transceivers. Then, the set of probabilities $\{p_i | i = 0, 1, \ldots, q-1\}$, corresponding to channels $\mathbb{F}$, is obtained following Definition 4. Based on $\{p_i | i = 0, 1, \ldots, q-1\}$, we get the value M so that $p_{M+1} \leq \bar{p} \leq p_M$. Then, the Prob-HP $\mathbb{S} = \{\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{q-1}\}$ could be obtained by the replacing algorithm, where $\mathbf{S}_k$ is the kth Prob-HP sequence.

The replacing algorithm can be described as follows: the channels $\{f_i, M+1 \leq i \leq q-1\}$ in $\{\mathbf{Q}_k\}_k$ are replaced by those slots $\{f_i, 0 \leq i \leq M\}$, so that the number of channels appearing in each sequence $\mathbf{S}_k, k = 0, 1, \ldots, q-1$ meets the given $\{p_i | i = 0, 1, \ldots, q-1\}$. Finally, the proposed Prob-HP is obtained.

It is well known that the detailed Prob-HP is determined by the specific replacing algorithm. The specific Prob-HP can be seen clearly by an example in the next subsection.

5 Examples of channel-hopping patterns and properties comparisons

In this section, we will present the examples of the channel-hopping patterns mentioned in the previous sections, particularly demonstrate the example of the proposed Prob-HP step by step. Then, the randomness and Hamming correlations of these example are studied.

5.1 Example of Prob-HP

Assuming that the probabilities of channels $\{f_i\}$ are obtained as follows based on the given channel gains $\{h_i\}$.

$$p_0 = 1/3, p_1 = 4/15, p_2 = 1/5, p_3 = 2/15, p_4 = 1/15. \tag{9}$$

The above probabilities imply that the channel f_4 has the poorest quality; thus, the usage probability is minimized. The channel f_0 has the best quality, so with the highest probability.

Based on the above probabilities, we set $q = 5$, the prime hopping pattern $\mathbb{P}$ is obtained as follows over the channel-slot set $\mathbb{F} = \{f_0, f_1, f_2, f_3, f_4\}$.

$$\mathbb{P} = \begin{Bmatrix} (0,1,2,3,4); \\ (0,2,4,1,3); \\ (0,3,1,4,2); \\ (0,4,3,2,1); \end{Bmatrix}. \tag{10}$$

Then, a new hopping pattern $\mathbb{Q}$ is obtained by the cascade operation of $m = 3$ terms of $\mathbb{P}$, i.e.,

$$\mathbb{Q} = [\mathbb{P}, \mathbb{P}, \mathbb{P}] := \{\mathbf{Q}_0, \mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3\}. \tag{11}$$

We can obtain that the probability of each channel in $\mathbf{Q}_k$ is $\bar{p} = 1/5$. The specific replacing scheme is shown in Fig. 1. According to this scheme, one of f_3 and one of f_4 in $\mathbf{Q}_k$ are replaced by f_0, and the other f_4 is replaced by f_1. Finally, the Prob-HP is obtained as

$$\mathbb{S} = \begin{Bmatrix} (0,1,2,0,4,0,1,2,3,0,0,1,2,3,1); \\ (0,2,4,1,0,0,2,0,1,3,0,2,1,1,3); \\ (0,0,1,4,2,0,3,1,0,2,0,3,1,4,2); \\ (0,4,0,2,1,0,0,3,2,1,0,1,3,2,1); \end{Bmatrix}. \tag{12}$$

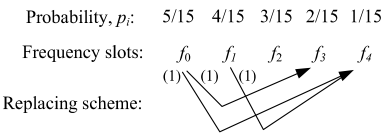

Fig. 1 A specific replacing algorithm of Prob-HP

5.2 Example of traditional NHZ hopping pattern

In this subsection, we will present an example of the traditional NHZ hopping pattern via the algorithm proposed in [34]. The parameters of algorithm are set as: $a_1 = 1, a_2 = 2, a_3 = 3$. The seed matrix is given by

$$\mathbb{C} = [(0,1,2,3,4)^T, (5,6,7,8,9)^T, (10,11,12,13,14)^T]. \tag{13}$$

Based on the seed matrix $\mathbb{C}$ and the parameters $\{a_i\}_i$, the traditional NHZ hopping pattern $\mathbb{S}_1(q,L,K,Z) = \mathbb{S}_1(15,15,5,2)$ is obtained as

$$\mathbb{S}_1 = \left\{ \begin{array}{l} (0,5,10,1,7,13,2,9,11,3,6,14,4,8,12); \\ (1,6,11,2,8,14,3,5,12,4,7,10,0,9,13); \\ (2,7,12,3,9,10,4,6,13,0,8,11,1,5,14); \\ (3,8,13,4,5,11,0,7,14,1,9,12,2,6,10); \\ (4,9,14,0,6,12,1,8,10,2,5,13,3,7,11); \end{array} \right\}. \tag{14}$$

5.3 Example of generalized NHZ hopping pattern

In this subsection, an example of generalized NHZ hopping pattern is presented, of which the construction algorithm has been proposed in [37]. The basic construction procedure of the generalized NHZ hopping pattern consists of two steps. Firstly, constructing multiple seed hopping patterns satisfying the Peng–Fan bound [33] and some specific requirements. Secondly, the constructed seed hopping pattern takes the interleaving operation. Here, we just present the brief construction procedure of the generalized NHZ hopping pattern.

Firstly, selecting three seed hopping patterns $\{\mathbb{C}^{(0)}, \mathbb{C}^{(1)}, \mathbb{C}^{(2)}\}$ over three non-overlapped channel-slot sets $\mathbb{F}^0 = \{0,1,2,3,4\}$, $\mathbb{F}^1 = \{5,6,7,8,9\}$ and $\mathbb{F}^2 = \{10,11,12,13,14\}$, respectively, where

$$\mathbb{C}^{(0)} = \{(1,1,2,4,2); (2,2,3,0,3); (3,3,4,1,4); (4,4,0,2,0); (0,0,1,3,1)\}$$
$$\mathbb{C}^{(1)} = \{(6,6,7,9,7); (7,7,8,5,8); (8,8,9,6,9); (9,9,5,7,5); (5,5,6,8,6)\}$$
$$\mathbb{C}^{(2)} = \{(11,11,12,14,12); (12,12,13,10,13); (13,13,14,11,14); (14,14,10,12,10); (10,10,11,13,11)\}.$$

It is easy to check that all hopping patterns $\{\mathbb{C}^{(0)}, \mathbb{C}^{(1)}, \mathbb{C}^{(2)}\}$ are optimal ones with respect to Peng–Fan bound.

Secondly, by the proposed interleaving algorithm, we can obtain the generalized NHZ hopping pattern $\mathbb{S}_2(q,L,K,Z,H_m) = \mathbb{S}_2(15,15,5,2,3)$ as follows

Table 1 The Hamming correlations of the proposed Prob-HP

τ	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7
Prob-HP															
$H_c(\tau)$	5	3	3	6	0	5	5	3	5	3	5	3	4	5	0
$H_a(\tau)$	1	2	10	2	2	1	2	15	2	1	2	2	10	2	1
Completely random															
$H_c(\tau)$	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
$H_a(\tau)$	3	3	3	3	3	3	3	15	3	3	3	3	3	3	3

Table 2 The Hamming correlations of the NHZ hopping patterns with Z=2

τ	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7
Gen. NHZ															
$H_c(\tau)$	0	3	0	0	3	0	0	0	0	0	3	0	0	3	0
$H_a(\tau)$	0	3	0	0	3	0	0	15	0	0	0	0	0	3	0
Trad. NHZ															
$H_c(\tau)$	0	5	0	0	5	0	0	0	0	0	5	0	0	5	0
$H_a(\tau)$	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0

$$\mathbb{S}_2 = \left\{ \begin{array}{l} (1,6,11,1,6,11,2,7,12,4,9,14,2,7,12); \\ (2,7,12,2,7,12,3,8,13,0,5,10,3,8,13); \\ (3,8,13,3,8,13,4,9,14,1,6,11,4,9,14); \\ (4,9,14,4,9,14,0,5,10,2,7,12,0,5,10); \\ (0,5,10,0,5,10,1,6,11,3,8,13,1,6,11). \end{array} \right\}. \tag{15}$$

5.4 Properties' comparisons

In this subsection, we will compare the Hamming cross- and auto-correlations of the aforementioned hopping patterns. For the fairness of comparisons, the parameters of hopping patterns (e.g., L and K) are set the same among these patterns.

Firstly, the Hamming cross- and auto-correlations of Prob-HP $\mathbb{S}$ are presented in Table 1. As the benchmark, the completely random hopping pattern is also shown in this Table. For the Prob-HP, the amount of channel hits is increased compared to the completely random hopping pattern, but the probability of each channel can be adjusted according to the channel qualities. As to the completely random hopping pattern, the amount of channel hits is identical for the various access delays, i.e., $H_c(\tau) = H_a(\tau) = 3$. By computing the probability of channel slot, the completely random hopping pattern has the identical usage probability $\{p_i\} = 1/5$, while the Prob-HP attains the various usage probabilities according to the channel qualities.

Secondly, the Hamming auto- and cross-correlations of traditional/generalized NHZ patterns are shown in Table 2. It is found that when the delay is constrained within the no-hit zone Z (i.e., $|\tau| \leq Z = 2$), the generalized NHZ hopping pattern maintains zero value of Hamming correlation as same as the traditional NHZ hopping pattern, while outside the no-hit-zone Z, the maximum cross-Hamming correlation is $H_m = 3$ which is lower than the traditional one ($H_m = 5$). The cost of optimal cross-correlation is the slight increase in auto-correlation, which results to the trivial effect on MAI of

multi-user systems. By computing the probability of channel, these two types of hopping patterns have the identical usage probability $\{p_i\} = 1/15$. Thus, these NHZ hopping patterns are the sort of the pseudo-random pattern.

By comparing Tables 1 and 2, it is observed that NHZ patterns can provide the orthogonality for the small access delay, but the Prob-HP cannot. The orthogonality is in favor of infrastructureless multi-node IoT system to completely avoid the multi-access interference (MAI). In addition, by comparing the examples of channel-hopping patterns as shown in (11), (14) and (15), it is found that the proposed Prob-HP can offer the specific usage probabilities matching to the channel qualities, but at the slight cost of degrading the uniformity of channel resource. Observed from the proposed construction of Prob-HP, the construction algorithm includes the nonlinear operations (e.g., replacing algorithm), which guarantees that Prob-HP is hard to be overheard and estimated by the eavesdroppers, while the most of conventional channel-hopping patterns (including NHZ patterns) are constructed by linear transformations.

6 Performance of wireless IoT based on proposed channel-hopping patterns under jamming attacks

In this section, the signal analysis will be conducted for the wireless IoT networks employing these types of hopping patterns in the presence of jamming attacks, which is helpful to evaluate the error-rate performance via simulations.

6.1 System model and signal analysis

A massive wireless IoT application (e.g., WiFi, Bluetooth, Zigbee and so forth) is congested within the limited ISM band, which cause severe interference and jamming attacks to the legitimate users. To reduce the impact of jamming/interference, the channel hopping is the common solution by avoiding the channel collisions between the legitimate one and the jammer/interference ones.

The channel-hopping transmission procedure can be modeled as the FH system. It is also well known that the WLAN standards (IEEE 802.11b/a/g) and Bluetooth standards utilize the FH technique as the basic transmission infrastructure. In this paper, we follow the FHMA system model with K legitimate users and one jammer, where the legitimate users transmit the signal via the hopped channels according to the proposed hopping pattern, whilst the jammer emits the attacking signal by specifically selecting the channels. For simplicity, we assume an M-ary FSK signal is sent by legitimate users and jammers during each hopping interval T. To avoid the inter-carrier interference of legitimate users, the minimum spacing of hopped frequency is assumed to be M/T. During each channel (i.e., frequency band in FH systems), we assume that the signal suffers from the flat Rayleigh fading as well as additive white Gaussian noise (AWGN) channel.

Before we analyze the signals, some definitions of the notations are firstly shown as follows.

- K: the amount of legitimate users in IoT networks. These users share the spectrum and avoid jamming attack by using the channel-hopping technique based on the proposed hopping patterns.

- $m^{(k)}(n)$: one M-ary symbol transmitted by the kth legitimate user during the nth hopping interval, which follows uniformly distributed over the alphabet set $\{0, 1, \ldots, M-1\}$.
- $s_n^{(k)}$: the instantaneous hopped channel of the kth legitimate user during the nth hopping interval, which depends on the assigned hopping pattern.
- η: is the complex AWGN with the two-sided power spectral density of $N_0/2$.
- $\sqrt{2P^{(k)}}$: the received signal amplitude of the kth legitimate user under the independent Rayleigh fading channel with the mean square value 2Ω.
- $\sqrt{2P^{(J)}}$: the signal amplitude of the jammer, which is also assumed to be the independent Rayleigh distribution with the mean square value $2\Omega_J$.
- $s_n^{(J)}$: the contaminated channel of the jammer during the nth interval, which depends on the scanning rule of jammer.
- τ_k: the relative access delay of the kth legitimate user caused by the transmission latency, synchronization attack and so forth. τ_k is assumed to be independently and uniformly distributed within $[-DT, DT]$, where D is the maximum delay.

Through the fading channel, the complex received signal during the nth hopping interval can be written as

$$r(t) = \sum_{k=1}^{K} \sqrt{2P^{(k)}} G_T(t - \tau_k - nT) \exp\left[j\left(2\pi \frac{m^{(k)}(n)}{T} t + 2\pi \frac{M}{T} t s_n^{(k)} + \varphi_n^{(k)} \right) \right] + \sqrt{2P^{(J)}} J(t) + \eta \tag{16}$$

where $\varphi_n^{(k)}$ denotes the random phase of the MFSK signal. $G_T(\cdot)$ is a unit rectangular pulse over an symbol interval T. $J(t)$ is the signal emitted from jammer, which is presented by the specific modulation signal imposed on the pseudo-random channel hopping.

In the legitimate receiver, the received signal is orderly put into dehopper, demodulation and decision blocks as shown in Fig. 1, where the non-coherent MFSK demodulator is adopted which is shown in [38]. Assuming the 1th user as the desired one, the decision variable in the lth branch of the matched filters observed during the nth interval is computed as (17) after some straightforward manipulation

$$|\Psi_l(n)| = \begin{cases} \left| \Gamma^{(1)} e^{j\varphi_n^{(1)}} + \sum_{k=2}^{K} I_l^{(k)}(n) + J'(t) + \nu_l \right|, & m^{(k)}(n) = l \\ \left| \sum_{k=2}^{K} I_l^{(k)}(n) + J'(t) + \nu_l \right|, & m^{(k)}(n) \neq l \end{cases} \tag{17}$$

where $\Gamma^{(k)}$ follows an i.i.d. Rayleigh distribution with probability density function (pdf) $f_{\Gamma^{(k)}}(x) = 2x \exp(-x^2)$ for $k = 1, 2, \ldots, K$. $I_l^{(k)}$ denotes as the MAI due to the kth interfering user. $J'(t)$ is the jamming signal. ν_l is a complex AWGN with mean zero and variance $\frac{1}{\overline{E}_s/N_0}$, where $\overline{E}_s = T\Omega$. Over the Rayleigh channels with jamming attack, it is found that the signal-to-jammer ratio is denoted as $SJR = \Omega/\Omega_J$. For the distinct channels, the values of Ω (or Ω_J) are a random variable followed by the Rayleigh distribution under the condition of the channel gains $\{h_i | i = 0, 1, 2, \ldots, q-1\}$.

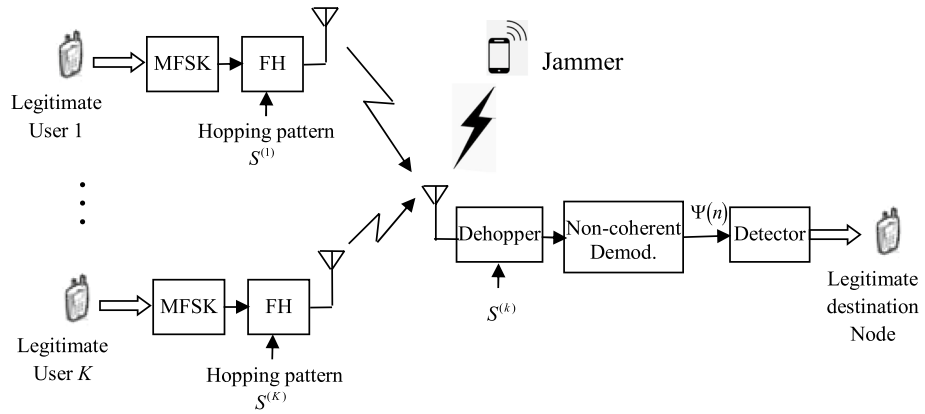

Fig. 2 The transceiver model of wireless IoT system based on channel hopping in the presence of jamming attacks

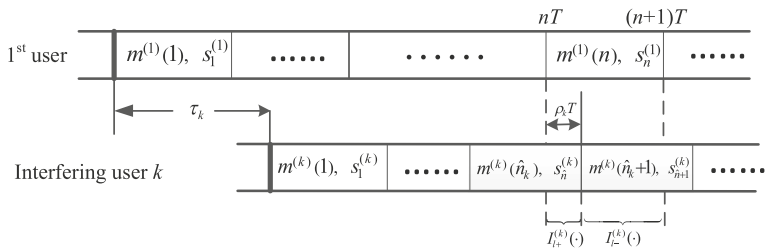

Fig. 3 The illustration of channel slots and MAIs between the 1st user and the interfering user k under time delay τ_k

In (17), the MAI and the jammer signal are the main impact factors on the transmission performance. Due to the applications of channel-hopping patterns, the MAI and the jamming attack can be efficiently reduced (Figs. 2, 3).

It is assumed that the access delay among the legitimate users τ_k is less than DT, which refers to the quasi-synchronous multiple access. Since τ_k follows the uniform distribution within $[-DT, DT]$, τ_k can be rewritten as $\tau_k = \Delta_k T + \rho_k T$, where the integer delay $\Delta_k = \lceil \tau_k / T \rceil$ and the normalized delay $\rho_k = \tau_k \mod T$. It is clear that Δ_k and ρ_k satisfy i.i.d. uniform distribution within $\{\lfloor -D/T \rfloor, \lfloor -D/T \rfloor + 1, \ldots, \lceil D/T \rceil - 1, \lceil D/T \rceil\}$ and [0,1), respectively. Thus, given a time delay τ_k of the kth user, the MAI $I_l^{(k)}(n)$ corresponding to the nth hopping interval $[nT, (n+1)T)$ shown in (17) can be evaluated in two subintervals: $I_{l+}^{(k)}$ for $nT \le t < nT + \rho_k T$ and $I_{l-}^{(k)}$ for $nT + \rho_k T \le t < (n+1)T$. That is [37],

$$I_l^{(k)}(n) = I_{l-}^{(k)}(n) + I_{l+}^{(k)}(n), \tag{18}$$

where

$$
\begin{aligned}
I_{l+}^{(k)}(n) &= h[s_{\hat{n}}^{(k)}, s_n^{(1)}]\Gamma^{(k)}\mathrm{sinc}(\rho_{\mathrm{k}}\theta_{\mathrm{l}-})\rho_{\mathrm{k}}\exp\left(\mathrm{j}(\pi\rho_{\mathrm{k}}\theta_{\mathrm{l}-}+\varphi^{(\mathrm{k})})\right),\\
I_{l-}^{(k)}(n) &= h[s_{\hat{n}+1}^{(k)}, s_n^{(1)}]\Gamma^{(k)}\mathrm{sinc}(\theta_{l+}(1-\rho_{\mathrm{k}}))(1-\rho_{\mathrm{k}})\\
&\quad\times\exp\left(j(\pi\theta_{l+}(\rho_k+1)+\varphi^{(k)}\right).
\end{aligned}
\tag{19}
$$

In the above equation, $\hat{n} = n + \Delta_k$ denotes the symbol interval index of the kth interfering user (which is obtained from the delay τ_k). $\varphi^{(k)}$ denotes the random phase of the MFSK signal. $\theta_{l-} = m^{(k)}(\hat{n}) - l$, and $\theta_{l+} = m^{(k)}(\hat{n}+1) - l$. The function $\mathrm{sinc(x)} = \sin(\pi \mathrm{x})/\pi \mathrm{x}$ if $x \neq 0$ and otherwise $\mathrm{sinc(x)} = 1$.

By using the aforementioned hopping patterns, the specific value of $h[s_{\hat{n}}^{(k)}, s_n^{(1)}]$ can be obtained. For the traditional and the generalized NHZ hopping patterns, when $|\tau_k| \leq ZT$ (i.e., under *quasi-synchronous* scenarios), we have $h[s_{\hat{n}}^{(k)}, s_n^{(1)}] \equiv 0$. For the generalized NHZ hopping pattern when $|\tau_k| > ZT$ (i.e., under *asynchronous* scenarios), the value of $h[s_{\hat{n}}^{(k)}, s_n^{(1)}]$ is minimized compared to the traditional NHZ hopping pattern, as shown in Table 2. For the proposed Prob-HP, the value of $h[s_{\hat{n}}^{(k)}, s_n^{(1)}]$ is also determined by the specific Hamming correlation property, as shown in Table 1. Note that for proposed Prob-HP $\mathbb{S}$ shown in (11), we have $\sum_{n=0}^{L} h[s_{\hat{n}}^{(k)}, s_n^{(1)}] \leq 6$ when $|\tau_k| \leq 5$ (i.e., under *quasi-synchronous* scenarios).

As for the jamming attacks, we assume the jammer also emits the MFSK signals by specially selecting the channels, where the rule of scanning channels of jammer is uniformly hopped over the q intended channels (q is equal to the size of the channels sets of legitimate user). Thus, the received jamming signal can be rewritten as

$$
\begin{aligned}
J'(t) &= h[s_{\hat{n}}^{(J)}, s_n^{(1)}]\mathrm{sinc}\left(\rho_{\mathrm{J}}\theta_{\mathrm{J}-}\right)\rho_{\mathrm{J}}\exp\left(\mathrm{j}(\pi\rho_{\mathrm{J}}\theta_{\mathrm{J}-}+\varphi^{(\mathrm{J})})\right)\\
&\quad+\ h[s_{\hat{n}+1}^{(J)}, s_n^{(1)}]\mathrm{sinc}\left(\theta_{\mathrm{J}+}(1-\rho_{\mathrm{J}})\right)(1-\rho_{\mathrm{J}})\exp\left(\mathrm{j}(\pi\theta_{\mathrm{J}+}(\rho_{\mathrm{J}}+1)+\varphi^{(\mathrm{J})})\right)
\end{aligned}
\tag{20}
$$

where the parameters $\{\rho_J, \theta_{J-}, \theta_{J+}, \varphi^{(J)}\}$ are same as those shown in (19), except that the values are dependent on the status of jammer. From the above equation, the probabilities of the events of $h[s_{\hat{n}}^{(J)}, s_n^{(1)}] = 1$ and $h[s_{\hat{n}+1}^{(J)}, s_n^{(1)}] = 1$, i.e., p_{J1} and p_{J2}, depend on the distributions of $s_{\hat{n}}^{(J)}$, $s_{\hat{n}+1}^{(J)}$ and $s_n^{(1)}$. With employing various hopping patterns mentioned in the previous sections, the value of $p_{J1,J2}$ is obtained as follows.

- Completely random hopping pattern: $p_{J1} = p_{J2} = 1/q$.
- Traditional NHZ hopping pattern: $p_{J1} = p_{J2} = 1/q$ since the each channel in NHZ hopping pattern follows the uniform distribution.
- Generalized NHZ hopping pattern: $p_{J1} = p_{J2} = 1/q$, of which reason is same as the traditional one.
- Probabilistic hopping pattern: the values of p_{J1} and p_{J2} are determined by the specific structure of the probabilistic hopping pattern.

The detector of receiver computes the M decision variables $|\Psi_l(n)|, l = 0, 1, \ldots, M-1$ and chooses the index of the largest decision variable as the estimate of the transmitted symbol, that is,

$$\hat{m}(n) = \arg\max_{l} |\Psi_l(n)|, \quad l = 0, 1, \ldots, M-1. \tag{21}$$

For the special case of $M = 2$, as $|\Psi_0(n)| > |\Psi_1(n)|$, the output of the detector is "0"; otherwise, it is "1". Based on (21), the BER of the wireless multi-user IoT system based on the specific channel-hopping patterns can be evaluated by Monte Carlo simulations later.

7 Simulations

In this section, we present the BER of wireless multi-user IoT networks employing the various hopping patterns in the presence of jamming attacks via Monte Carlo simulations. For the convenient comparisons, the parameters of the adopted channel-hopping patterns are set to the same with each other. The examples of these channel-hopping patterns are shown in the previous sections. Besides, the wireless channels are assumed to be the flat Rayleigh fading with $E\{\Gamma^{(k)}\} = 1$.

7.1 BER versus *K*

The BERs of the channel-hopping-based wireless multi-user IoT networks for various number of legitimate users K are shown in Fig. 4. The traditional/generalized NHZ hopping patterns are $\mathbb{S}_1(q, M, L, Z) = \mathbb{S}_1(15, 5, 15, 2)$ and $\mathbb{S}_2(q, M, L, Z, H_m) = \mathbb{S}_2(15, 5, 15, 2, 3)$, respectively. In this simulation, the maximum delay is set as $D = 4$ and the signal-to-jamming ratio SJR $= 0$ dB. The curves agree with the common behavior that the BER degrades with increasing K. For the case of single user ($K = 1$), the probabilistic hopping pattern outperforms other patterns. For the large K, its performance gets worse against the others. This phenomenon is due to the fact that, with increasing K, MAI becomes the dominate factor for performance degradations and the Hamming cross-correlation property of Prob-HP is the worst one among these patterns, as shown in Tables 1 and 2. Besides, the BER of generalized

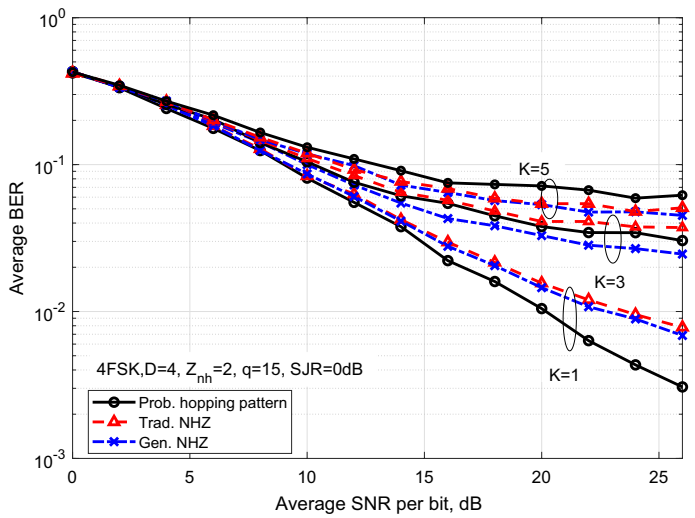

Fig. 4 The BERs of the channel-hopping-based wireless multi-node IoT networks for various number of legitimate users *K*

NHZ pattern is slightly better than that of traditional NHZ pattern, due to the lower value of Hamming correlation as shown in Table 2.

7.2 BER versus SJR for the single legitimate user

The BERs of the channel-hopping-based wireless multi-user IoT networks for various SJRs with $K = 1$ are shown in Fig. 5. For the case when $K = 1$, the jamming attack is the main impact on the performance. From this figure, the BER increases with the decrease of SJR since the jamming power increases. Compared to the (generalized) NHZ hopping patterns, the Prob-HP attains the best error rate. The reason lies in that the Prob-HP has the lower usage probability with regard to the channels attacked by the jammer, while the high usage probability for the other channels.

7.3 BER versus SJR for the multiple legitimate users

The BERs of the channel-hopping-based wireless multi-user IoT networks for various SJRs with multiple legitimate users ($K = 3$) are shown in Fig. 5. In this figure, the MAI and jamming attack are imposed into the wireless communication networks. For the large value of SJR, e.g., SJR = 0 dB, the curve of Prob-HP lies in the middle position of traditional NHZ and generalized NHZ patterns. As increasing SJR, the jamming attack becomes the main factor on the error rate other than MAI; thus, the BER of Prob-HP is the lowest one among these hopping patterns.

From Figs. 4 and 6, we observe that the traditional/generalized NHZ hopping patterns possess the unique advantage to combat the mutual interference contributed from other legitimate users, but with poor capability to avoid the jamming attacks. The Prob-HP behaves conversely, that is, it has the superiority in avoiding the jamming attack but with the poor capability of anti-interference.

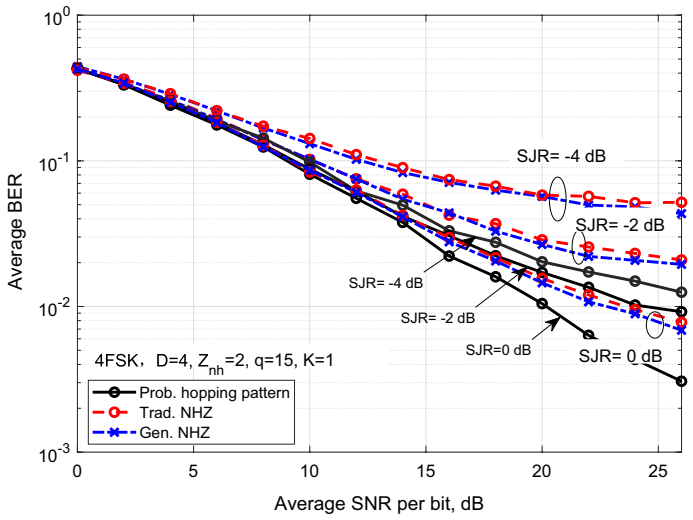

Fig. 5 The BERs of the channel-hopping-based wireless multi-node IoT networks for various *SJR*s with $K = 1$

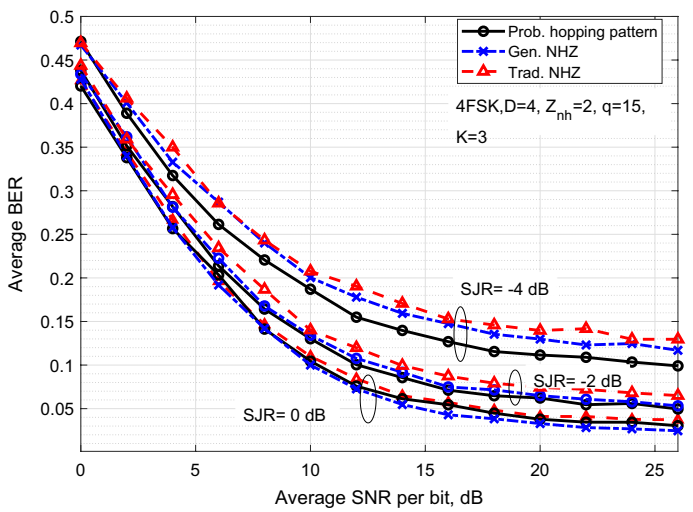

Fig. 6 The BERs of the channel-hopping-based wireless multi-node IoT networks for various *SJR*s with multiple legitimate users ($K = 3$)

8 Results and discussion

8.1 Results

In this paper, we have focused on the channel-hopping pattern-based multi-node IoT networks in smart cities for reducing both the mutual interference and the external jamming attacks. To achieve the goal, we have introduced several promising hopping patterns, i.e., traditional NHZ and the generalized NHZ patterns as well as proposed the new Prob-HP. The construction algorithm of Prob-HP was presented and demonstrated by the step-to-step example. The critical properties of hopping patterns, e.g., Hamming correlations and uniformity, were analyzed, which are important to the capacity of combating interference and jamming attack. Observed from the properties, the traditional/generalized NHZ hopping patterns have the quasi-orthogonality of Hamming correlations, which imply that there are less channel hits (even collision-free) for the multiple legitimate users access. For the Prob-HP, the usage probabilities of channels match to the occurrence probabilities of jamming attack on such channels. The Prob-HP possess merits for actively avoiding the jamming attack.

As a case study, the multiple legitimate users in the IoT networks are assumed to send the MFSK signals by using the proposed hopping patterns. The BER performance of such networks in the presence of jamming attack has been investigated. By the simulations, some interesting conclusions can be drawn. The traditional and generalized NHZ hopping patterns have the lower BER in the case of the massive legitimate users, but with poor capability to combat the jamming attack. The Prob-HP has the opposite behaviors, that is, it has the superiority in the presence of strong jamming attack but with relatively poor anti-MAI capability. These BER phenomena can be also verified by the Hamming correlations and randomness properties of the hopping patterns.

8.2 Discussion

Time hopping/frequency hopping is the basic technique in IoT communication networks for suppressing denial-of-service attacks (e.g., the mutual interference and jamming attacks) in the physical layer. The hopping pattern is the most critical component in TH/FH systems. The traditional/generalized NHZ hopping patterns and Prob-HP discussed in this paper can be conveniently deployed in IoT-based smart cities applications and provide favorable merits to guarantee the transmission security and performance. However, it is noted that, in the channel-hopping-based IoT networks, the number of nodes accommodated in IoT networks is strictly subject to the number of channel resources. One of potential solutions is to combine the new multi-access scheme (for example, non-orthogonal multi-access) into channel-hopping systems to support the massive connectivity. In addition, the performance of the IoT networks is investigated by semi-analysis and semi-simulation methods in this paper, and the theoretical performance integrating with the security policies in the upper layers with regard to the channel-hopping-based IoT networks still remains open issue, which will be our future works.

Abbreviations

IoT: Internet-of-thing; WLAN: Wireless local area network; NHZ: No-hit-zone; WiFi: Wireless fidelity; ISM: Industrial–scientific–medical; FH: Frequency-hopping; TH: Time-hopping; MAI: Multi-access interference; FSK: Frequency-shift keying modulation; Prob-HP: Probabilistic hopping pattern; AWGN: Additive white Gaussian noise; BER: Bit error rate; SJR: Signal-to-jamming ratio.

Acknowledgements

Not applicable.

Authors' contributions

YL and YZ conceived of the solution of the hopping patterns to the cyber-security issue in the IoT-based smart cities and carried out the designs of the multiple hopping patterns, participated in the system analysis and drafted the manuscript. QZ participated in the traditional and generalized NHZ patterns designs, conducted the signal processing of IoT networks and helped to draft the manuscript. KW and YH partly participated in MATLAB simulations with regard to the error rate of IoT systems. All authors read and approved the final manuscript.

Funding

This work is supported in part by Sichuan Province Science and Technology Support Program under Grant 2020YFG0292.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

All authors read and approved the final manuscript.

Competing interests

The affiliations of authors claim that the results and the analysis methodologies in this paper will not be implemented into productions and will not be applied into the patent.

Author details

[1]Science and Technology on Communication Security Laboratory, Chengdu, China. [2]China Electronics Technology Cyber Security Co., Ltd, Chengdu, China. [3]College of Electrical Engineering, Sichuan University, Chengdu, China.

Received: 12 January 2021 Accepted: 1 July 2021
Published online: 13 July 2021

References

1. A. Gharaibeh, M.A. Salahuddin, S.J. Hussini, A. Khreishah et al., Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun. Surv. Tutor. **19**, 2456–2501 (2017)
2. S. Liu, X. Liu, S. Wang, K. Muhammad, Fuzzy-aided solution for out-of-view challenge in visual tracking under IoT assisted complex environment. Neural Comput. Appl. **33**, 1055–1065 (2021)
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi et al., Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**, 2347–2376 (2015)
4. K. Zhang, J. Ni, K. Yang, X. Liang et al., Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **1**, 122–129 (2017)
5. A.D. Didolkar, F.I.Z. Zama, SMARTIE: a security solution for a smart city using internet of things-architecture reference model. Int. J. Adv. Res. Innov. Ideas Educ. **2**, 1–6 (2016)
6. K. Ren, Q. Wang, C. Wang, Z. Qin, X. Lin, The security of autonomous driving: threats, defenses, and future directions. Proc. IEEE **8**(2), 357–372 (2020)
7. Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, K. Ren, Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy. IEEE Trans. Dependable Secure Comput. **15**(4), 591–606 (2018)
8. L. Zhao, S. Hu, Q. Wang, J. Jiang, C. Shen, X. Luo, P. Hu, Shielding collaborative learning: mitigating poisoning attacks through client-side detection. IEEE Trans. Depend. Secure Comput. (**Early access**)
9. Y. Zhao, Y. Yang, B. Tian, T. Zhang, An invocation chain test and evaluation method for fog computing. I. Wirel. Commun. Mobile Comput. **2020**, 1–11 (2020)
10. Y. Yu, L. Tan, M. Aloqaily, H. Yang, Y. Jararweh, Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans. Ind. Inform. **(Early access)**
11. Bluetooth Special Interest Group (SIG): Bluetooth Specification, 683 Version 5.0 (2016). http://www.bluetooth.org. Accessed 31 Dec 2016
12. X. Wang, Z. Liu, Y. Gao et al., A near-optimal protocol for the grouping problem in RFID systems. IEEE Trans. Mobile Comput. **20**, 1257–1272 (2019)
13. S. Liu, C. Guo, F. Al-Turjman et al., Reliability of response region: a novel mechanism in visual tracking by edge computing for IIoT environments. Mech. Syst. Signal Process. **138**, 1–15 (2020)
14. K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Surv. Tutor. **13**, 245–257 (2011)
15. Q. Wang, T. Nguyen, K. Pham, H. Kwon, Mitigating jamming attack: a game-theoretic perspective. IEEE Trans. Veh. Technol. **67**, 6063–6074 (2018)
16. C. Kolias, G. Kambourakis, S. Gritzalis, Attacks and countermeasures on 802.16: analysis and assessment. IEEE Commun. Surv. Tutor. **15**, 6487–514 (2013)
17. N. Nishanth, A. Mujeeb, Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Syst. J. (**Early access**)
18. L. Jia, Y. Xu, Y. Sun, S. Feng, A. Anpalagan, Stackelberg game approaches for anti-jamming defence in wireless networks. IEEE Wirel. Commun. **25**, 120–128 (2018)
19. Y. Wu, B. Wang, K.J.R. Liu, T.C. Clancy, Anti-jamming games in multi-channel cognitive radio networks. IEEE J. Sel. Areas Commun. **30**, 4–15 (2012)
20. M. Letafati, A. Kuhestani, H. Behroozi, D.W.K. Ng, Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay. IEEE Trans. Commun. **19**, 6771–6785 (2020)
21. Chao, C.M., Lee, W.C., Wang, C.X., et al: A flexible anti-jamming channel hopping for cognitive radio networkss, in *2018 6th International Symposium on Computing and Networking Workshops: 27–30 Nov 2018, Takayama*, ed. by C.M. Chao (2018), pp. 1–6
22. J. Jeung, S. Jeong, J. Lim, Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN, in *The 2011 Military Communications Conference: 7-11 Nov 2011, Baltimore*, ed. by C.M. Chao (2011), pp. 1–6
23. C. Li, P. Qi, D. Wang et al., On the anti-interference tolerance of cognitive frequency hopping communication systems. IEEE Trans. Reliab. (Early Access) 1–12(2021)
24. Y. Zhao, X. Fang, Z. Zhao, Interference coordination in compact frequency reuse for multihop cellular networks. IEICE Trans. Fund. Electron. **93-A**, 2312–2319 (2010)
25. Y. Zhao, X. Fang, R. Huang, Y. Fang, Joint interference coordination and load balancing for OFDMA multi-hop cellular networks. IEEE Trans. Mobile Comput. **13**, 89–101 (2014)
26. S. Liu, S. Wang, X. Liu et al., Fuzzy detection aided real-time and robust visual tracking under complex environments. IEEE Trans. Fuzzy Syst. **29**, 90–102 (2021)
27. S.W. Golomb, G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications* (Cambridge University Press, Cambridge, 2005)
28. J. Bao, L. Ji, New families of optimal frequency hopping sequence sets. IEEE Trans. Inf. Theory **62**, 5209–5224 (2016)
29. J.H. Chung, G. Gong, K. Yang, New families of optimal frequency-hopping sequences of composite lengths. IEEE Trans. Inf. Theory **60**, 3688–3697 (2014)
30. Z. Zhou, X. Tang, D. Peng, U. Parampalli, New constructions for optimal sets of frequency-hopping sequences. IEEE Trans. Inf. Theory **57**, 3831–3840 (2011)
31. P. Fan, M.H. Lee, D. Peng, New family of hopping sequences for time/frequency-hopping CDMA systems. IEEE Trans. Wirel. Commun. **4**, 2836–2842 (2005)
32. A. Lempel, H. Greenbergerg, Families of sequences with optimal hamming correlation properties. IEEE Trans. Inf. Theory IT **20**, 90–94 (1974)
33. D.Y. Peng, P.Z. Fan, Lower bounds on the hamming auto- and cross correlations of frequency-hopping sequences. IEEE Trans. Inf. Theory **50**, 2149–2153 (2004)
34. W.X. Ye, P.Z. Fan, E.M. Gabidulin, Construction of non-repeating frequency-hopping sequences with no-hit zone. Electron. Lett. **42**, 681–682 (2006)

35. X. Liu, L. Zhou, Q. Zeng, No-hit-zone frequency hopping sequence sets with respect to aperiodic hamming correlation. Electron. Lett. **54**, 212–213 (2018)
36. Q. Zeng, X. Liu, P.F. Du, Multi-level sequence-based frequency-hopping in multi-cell networks. IEEE Trans. Veh. Technol. **69**, 16282–16287 (2020)
37. Q. Zeng, Z.Z. Zhou, X. Liu, Z.L. Liu, Strong no-hit-zone sequences for improved quasi-orthogonal FHMA systems: sequence design and performance analysis. IEEE Trans. Commun. **67**, 5336–5345 (2019)
38. M.K. Simon et al., *Spread Spectrum Communications Handbook* (McGraw-Hill, New York, 2001)

Publisher's Note