Journal of Southeast University (English Edition) Vol. 20 No. 4 Dec. 2004 ISSN 1003—7985

Novel method of enhancing the key amount for FH systems

Shen Fei Song Tiecheng Ye Zhihui Liu Tong Xia Weiwei

(National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

Abstract: Based on the principle of information theory, a novel scheme of unequal-interval frequency-hopping (FH) systems is proposed. For cases of spectrum overlapping systems and non-overlapping systems, the implementation methods are presented and the security performances are discussed theoretically. Firstly, the definitions of absolute and relative key amounts of FH systems, equal-interval and unequal-interval FH systems are given. Then, the absolute key amount and relative key amount are analyzed for equal-interval and unequal-interval FH systems. The results indicate that the absolute key amount has become the key point in improving the security and secrecy of FH systems, especially in today's epoch of highly developed computer science and IC design technology. Theoretical analysis and practical examples show that the absolute key amount of unequal-interval FH systems is generally over two orders larger than that of equal-interval ones when spectrum overlapping is allowable. Therefore, there is great superiority in enhancing the security and secrecy for the scheme mentioned.

Key words: frequency-hopping system; key amount; security of information; unequal-interval carriers; frequency-shift filter

Frequency-hopping (FH) communication systems provide high performances in secrecy, anti-interception, anti-jamming and spectrum efficiency. Therefore, FH communication schemes show great superiority in both military and business uses. The FH technology is increasingly being used with the opening of the industry, science and medicine (ISM) band in many countries. Furthermore, it has become the key technology in Bluetooth, IEEE 802.11, IEEE 802.15, HomeRF and many other communication systems[1-6].

The effect of spread spectrum for FH system is accomplished by hopping carriers so that the process gain is decided by both the number of carrier frequencies (channels) for a given band and the effective width of each channel. Therefore, it is a macro-wideband system as well as a micro-narrowband system. Generally, in spread spectrum, the more channels, the greater gains can be achieved.

Among the many characteristics of FH systems, secrecy and the information rate which are closely related to each other are of greatest concern. The performance of the secrecy of an FH system is often measured by its key amount[7], the number of carriers and the hopping rate. The larger the key amount, the more the carriers and the quicker the hopping rate, the better the secrecy will be. The most widely used way of achieving FH is to use a phase-locked loop (PLL) frequency synthesizer in order to reduce the cost of equipment. And the bottleneck of increasing the rate of information transmission is the setup time of PLL when the carrier is changed. In many practical systems, the definite number of channels and the known interval between carriers are provided. This is called an equal-interval FH system. In this case, the requirement for setup time has to be relaxed so as to realize the systems easily, which causes a decrease in the information transmission rate. For example, in the 79-channel-Bluetooth with 1 MHz interval of each channel, which $f_k = (2\,402 + k)$ MHz, $k = 0, 1, 2, \cdots, 78$, the time length of a single slot packet is 625 μs and the time of sending data or receiving data is only 366 μs at most. It is clear that the ratio of time left to setup is as high as 42%. Although equal-interval FH and such long setup time can be allowed in some application occasions, they are unacceptable in those fast application situations that require great secrecy and wideband. In this paper, the factors influencing the key amount of FH systems are firstly analyzed theoretically, and then a novel scheme that can largely enhance the key amount and reduce the setup time of PLL frequency synthesizer is presented. Finally, the analysis of their performance and some application instances are provided. The methods mentioned in this paper are already in the patent application process.

Received 2004-09-15.

Foundation items: The National Natural Science Foundation of China (No. 60072016), the National High Technology Research and Development Program of China (863 Program) (No.2003AA1Z1110), the High Technology Research and Development Program of Jiangsu Province (No.BG2003004), the Key Project of Science and Technology of Ministry of Education (02171).

Biographies: Shen Fei (1983—), female, undergraduate; Song Tiecheng (corresponding author), male, professor, songtc@seu.edu.cn.

1 Analysis of Key Amount for FH Systems

Some definitions are provided as follows for easy analysis.

Definition 1 For N as the total number of carrier frequencies available in an FH system, the information required to decide all the elements of its carrier frequency set $\{f_1, f_2, \cdots, f_{i-1}, f_i, \cdots, f_{N-1}, f_N\}$ is defined as the system's absolute key amount E_a.

Definition 2 For N as the total number of carrier frequencies available in the FH system, the information required to decide the hopping rule of K elements of the carriers set $\{f_1, f_2, \cdots, f_{i-1}, f_i, f_{i+1}, \cdots, f_{K-1}, f_K\}$, which is used in practical communication, is defined as the FH system's relative key amount E_r.

Definition 3 For the given frequency band $[f_L, f_H]$, suppose N is the total number of carrier frequencies available in the FH system. In the carriers set $\{f_1, f_2, \cdots, f_{i-1}, f_i, f_{i+1}, \cdots, f_{N-1}, f_N\}$, if there is $f_i - f_{i-1} = f_{i+1} - f_i$ for any i, $i \in [1, N]$ and $f_0 = f_L$, $f_{N+1} = f_H$, then this FH system is defined as the equal-interval FH system.

Definition 4 For the given frequency band $[f_L, f_H]$ in an FH system, set M as the total number of carrier frequencies available. In the carrier frequencies set $\{f_1, f_2, \cdots, f_{j-1}, f_j, f_{j+1}, \cdots, f_{M-1}, f_M\}$, if there is either $f_j - f_{j-1} = f_{j+1} - f_j$ or $f_j - f_{j-1} \neq f_{j+1} - f_j$ for any j, $j \in [1, M]$ and $f_0 = f_L, f_{M+1} = f_H$, then it is defined as an unequal-interval FH system.

Now let's discuss the absolute and relative key amounts for equal-interval and unequal-interval FH systems, respectively.

For an equal-interval FH system, one can get its absolute key amount as long as he or she gets its total number N of carrier frequencies and any two neighboring carriers. In order to illuminate the principle, propose that only N is given, and then according to definition 1, the absolute key amount E_{a1} is

$$E_{a1} = 2\log_2 N \tag{1}$$

Considering the system of Bluetooth with 79 carrier frequencies and equal-interval FH, its absolute key amount is about 12.6 bits.

For the unequal-interval FH system, one cannot get the absolute key amount unless he or she acquires all the carrier frequencies, that is, all the elements of the carrier frequencies set. According to definition 1, while given merely the total number N of carrier frequencies of the unequal-interval FH system, its absolute key amount E_{a2} can also be gotten as

$$E_{a2} = N\log_2 N \tag{2}$$

Now consider the Bluetooth system if it were an unequal-interval FH system. Though the system also has 79 carrier frequencies, its absolute key amount is about 498 bits, which is $N/2 = 39.5$ times larger than that of the equal-interval FH system. From the reasoning above, a conclusion can be reached that the absolute key amount of unequal-interval FH systems is far larger than that of equal-interval FH systems when using the same amount of carriers.

The FH systems avoid interruptions and interceptions by changing carriers very quickly when they are in communication. The pattern based on the pseudo-noise sequence (PN code) is used to achieve the frequency, hopping and frequency hopping code division multiple access (FH-CDMA). The period of the FH pattern is easy to lengthen. For a binary system, proposing that i bits are required to decide the FH pattern and according to definition 2, the relative key amount is

$$E_r = 2^i \log_2 2^i = i \cdot 2^i \tag{3}$$

For example, the FH pattern in Bluetooth is decided by both 28 bits of its clock timer and 28 bits of its address code. According to definition 2 and Eq. (3), its relative key amount is as high as 56×2^{56} bits.

Since the FH pattern is merely determined by the method of generating PN code, equal-interval FH and unequal-interval FH exert no direct influence on their relative key amounts.

From the aforementioned reasoning, we can conclude that the relative key amount of FH systems is far larger than the absolute key amount. Hence, the latter one is highlighted in this paper. From definition 1, the total number of carrier frequencies for FH systems directly determines the system's absolute key amount. The reasons are as follows: from the view of information safety, if using some receivers working on a per channel basis, that is, all channels are monitored, all information in communication will be captured no matter how long the period of the FH pattern or how high its relative key amount is. As a result, only if both the relative and absolute key amounts are high enough can the FH system be secure and secret.

Moreover, a conclusion can be reached from the reasoning above that the absolute key amount of unequal-interval FH systems is far larger than that of equal-interval systems. Actually, since the elements of the set of equal-interval FH systems disperse equidistantly on the frequency axis, while those of the set of unequal-interval FH systems are of an approximately continuous distribution, the absolute key amount of practical unequal-interval FH systems will be even larger.

2 Descriptions and Realization of the Frequency Set Available

For a given frequency band $[f_L, f_H]$, let the first and last carrier frequency of equal-interval FH systems be $f_{c,1}$, $f_{c,N}$, respectively, the interval of neighboring carrier frequencies be f_{span}, the effective bandwidth of modulated signal be B. If it is required to work under FH-CDMA and have no collision or overlap of frequency spectrum, it should satisfy the equations as follows:

$$f_{c,1} \geqslant f_L + B/2$$
$$f_{c,N} \leqslant f_H - B/2$$

Now any element $f_{c,i}$ of its carrier frequency set can be represented as

$$f_{c,i} = f_{c,1} + (i-1) f_{span} \qquad i \in [1, N] \tag{4}$$

It is easy to get all the elements of the set $\{f_{c,1}, f_{c,2}, \cdots, f_{c,i-1}, f_{c,i}, f_{c,i+1}, \cdots, f_{c,N-1}, f_{c,N}\}$ by adducing Eq. (4). It is convenient to get the needed carrier frequency by using the frequency synthesizer shown in Fig.1. Here

$$f_{PD} = f_{out}/N = f_{ref}/R \tag{5}$$

is the phase-detected frequency and generally $f_{PD} = f_{span}$. Setting a fixed frequency division ratio R for the output frequency f_{ref} which is generated by the reference oscillator and changing N, the output frequency f_{out} generated by the voltage-controlled oscillator (VCO) can be equal to $f_{c,i}$.

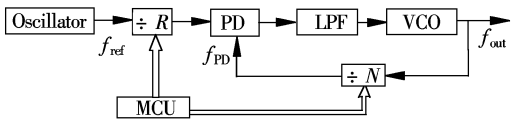

Fig.1 Phase-locked loop frequency synthesizer

For unequal-interval FH systems, the set of carrier frequencies $\{f_{c,1}, f_{c,2}, \cdots, f_{c,j-1}, f_{c,j}, f_{c,j+1}, \cdots, f_{c,N-1}, f_{c,N}\}$ is accompanied with its interval set $\{f_{span,1}, f_{span,2}, \cdots, f_{span,j-1}, f_{span,j}, f_{span,j+1}, \cdots, f_{span,N-1}, f_{span,N}, f_{span,N+1}\}$, where $f_{span,1} = f_{c,1} - f_L$, $f_{span,2} = f_{c,2} - f_{c,1}$, $\cdots$, $f_{span,j} = f_{c,j} - f_{c,j-1}$, $\cdots$, $f_{span,N} = f_{c,N} - f_{c,N-1}$, $f_{span,N+1} = f_H - f_{c,N}$. Fig. 2 is a sketch map about the arrangement of the carrier frequencies set for the unequal-interval FH system on the frequency axis.

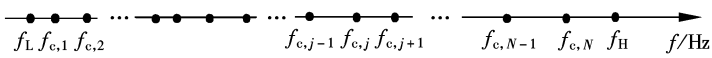

Fig.2 Sketch map of array relation of carrier frequencies for the unequal-interval FH system

Let Δf be the greatest common divisor of all the elements of the interval set. There is

$$\Delta f = \mathrm{GCD}\{f_{span,1}, f_{span,2}, \cdots, f_{span,j-1}, f_{span,j}, f_{span,j+1}, \cdots, f_{span,N-1}, f_{span,N}, f_{span,N+1}\} = (\{f_{span,1}, f_{span,2}, \cdots, f_{span,j-1}, f_{span,j}, f_{span,j+1}, \cdots, f_{span,N-1}, f_{span,N}, f_{span,N+1}\}) \tag{6}$$

Then each element $f_{c,j}$ in the set of carrier frequencies can be described as

$$f_{c,j} = f_L + \sum_{j=1}^{N} k_j \Delta f \tag{7}$$

where

$$k_j \Delta f = f_{span,j} = f_{c,j} - f_{c,j-1} \tag{8}$$

If k_j is a random natural number generated by the random natural number generator, then the sequence calculated from Eq.(7) is the carrier frequencies set of the unequal-interval FH that is shown in Fig.2.

Similar to the case of equal-interval FH, set the effective bandwidth of modulated signal as B, and no channels collision or frequency overlap is required under FH-CDMA, the carrier intervals of unequal-interval FH systems should satisfy

$$f_{span,1} = f_{c,1} - f_L = k_1 \Delta f \geqslant B/2 \tag{9}$$
$$f_{span,j} = f_{c,j} - f_{c,j-1} = k_j \Delta f \geqslant B \tag{10}$$
$$f_{span,N+1} = f_H - f_{c,N} = k_{N+1} \Delta f \geqslant B/2 \tag{11}$$

The minimum k_{min} of the random k_j from Eqs.(9) to (11) can be elicited. And there should be $k_1 \geqslant k_{min}$, $k_i \geqslant 2k_{min}$, $k_N \geqslant k_{min}$. A maximum k_{max} can also be set in order to avoid a too large k_j and to keep a balance between the randomicity of k_j and the spectrum efficiency, so that

$$k_{min} \leqslant k_1, \ k_{N+1} \leqslant k_{max} \tag{12}$$
$$2k_{min} \leqslant k_j \leqslant k_{max} \qquad j = 1, 2, \cdots, N-1 \tag{13}$$

Eqs.(6) to (13) are the theoretical algorithms to get the carrier frequencies set for the unequal-interval FH system. However, it is very difficult to get the accurate solution to this set from Eqs.(6) to (11), since Eqs.(7) to (11) are all based on Δf while Δf itself is based on Eq. (6). It is not necessary to use such an intricate iterative method in practice. So a relatively simple method is presented as follows. A relatively small Δf and proper k_{min} and k_{max} are set up first and then the elements of the set are calculated according to Eqs. (7) to (13). Finally, the results will be evaluated. The values of Δf, k_{min} and k_{max} will be adjusted and the equations will be recalculated until getting the satisfying carrier frequencies set. Fig. 3 shows the flow chart for getting all the elements of the set. It can be conveniently fulfilled by computer or microprocessors.

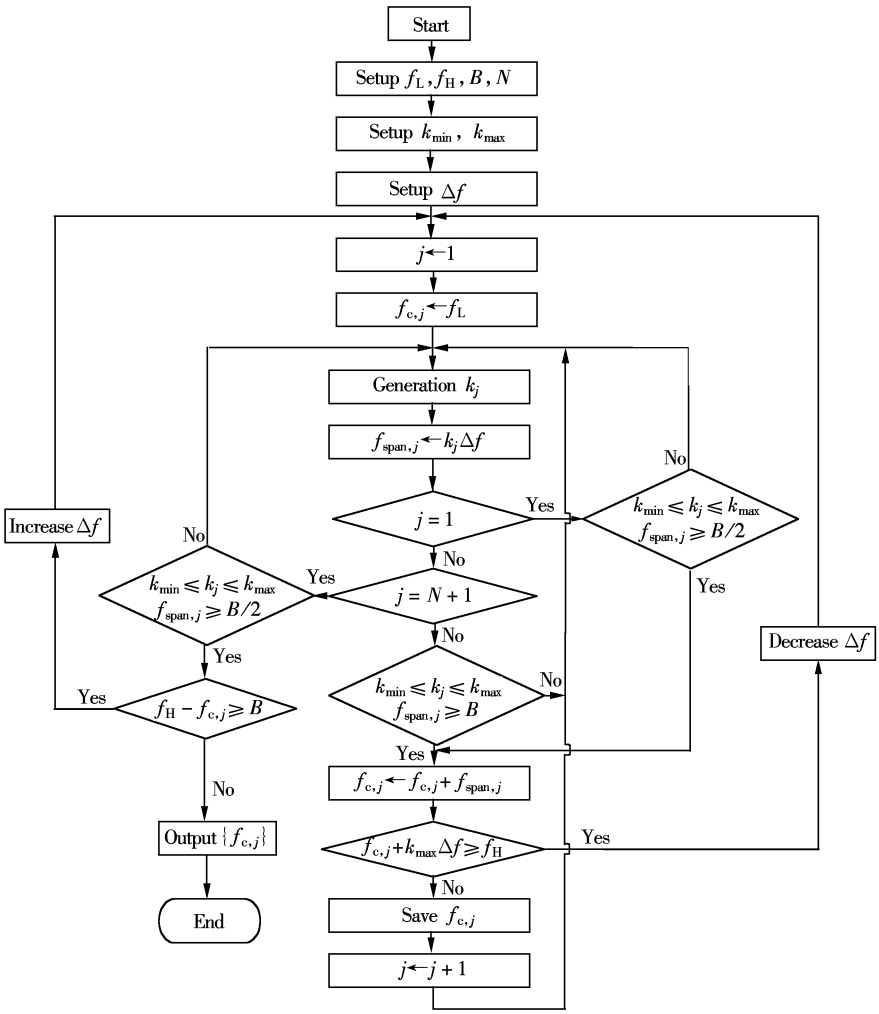

Fig.3 Flow chart for getting all the elements of the set for the unequal-interval FH system

3 Further Analysis of the Absolute Key Amount

When reexamining Eqs. (1) and (2), it is quite clear that when using the same N carrier frequencies, the reason why the absolute key amount of the unequal-interval FH system is $N/2$ times larger than that of the equal-interval FH is that every carrier frequency of the former system must be determined independently while the elements of the latter system are related to each other. When referring to information theory[8], it is obvious that the information needed by the former set is greater than the latter. Actually, most modulated signals have the performance of cyclostationarity, so that it is not necessary to require a B as the minimum interval between neighboring channels. In other words, when setting B as the effective bandwidth of modulated signals, spectrum overlap is allowable when working under FH-CDMA with no collision or "hit". The useful information can be extracted by using the frequency shift filter as long as there are distinguishing intervals in the carriers[9]. The absolute key amount of the unequal-interval FH system will be even larger if using this character. So the FH systems can be classified into overlap allowable systems and overlap unallowable systems according to whether overlaps are allowable under multiple accesses. It will be discussed concretely as follows.

Firstly, the situation of using the full band of $[f_H, f_L]$ is discussed.

The most common situation should be $NB = f_H - f_L$. So it can only be equal-interval in overlap unallowable systems.

In overlap allowable systems, let's consider the equal-interval systems first. Suppose the actual carrier interval is B'. Then the total number of carriers that can be held in $[f_H, f_L]$ will increase to N'_1 from N

$$N'_1 = (f_H - f_L)/B' \tag{14}$$

The absolute key amount will increase accordingly to

$$E_{a1} = 2\log_2 N'_1 \tag{15}$$

Its increment is

$$\Delta E_{a1} = 2\log_2 (N'_1/N) \tag{16}$$

Compared with the Bluetooth example above, where

the absolute key amount for FH is about 12.6 bits when $B = 1$ MHz and $N = 79$, it is clear that in overlap allowable systems, if $B' = 0.2$ MHz, $N'_1 = 395$. Now its absolute key amount is about 17.3 bits with an increment of about 4.6 bits.

Then consider the unequal-interval FH system. If the overlap spectrum is allowable and other conditions are the same as the equal-interval FH system, its absolute key amount will increase as well to

$$E_{a2} = N' \log_2 N'_2 \tag{17}$$

Its increment is

$$\Delta E_{a2} = N'_2 \log_2 (N'_2/N) \tag{18}$$

However, since now there must be many carrier intervals larger than B', there must be $N'_2 < N'_1$ accordingly. Take the frequency segment for Bluetooth as an example again. When $B' = 0.2$ MHz, if $N'_2 = 200$, the absolute key amount is about 1 528.8 bits with an increment of about 1 030.8 bits.

Then, the situation of $NB < f_H - f_L$ is discussed.

This situation is very common in ISM. For instance, in ISM 2 400 to 2 483.5 MHz, the carrier of Bluetooth is $f_k = (2\ 402 + k)$ MHz, where $k = 0, 1, 2, \cdots, 78$. We can still add 4 carriers into this frequency segment since the bandwidth of signal is 1 MHz. What is more, in the frequency segment of 902 to 928 MHz and 5 725 to 5 850 MHz, many FH communication systems use merely a tiny part of the band.

In overlap unallowable systems, the total number of carriers for equal-interval FH system will be

$$N'_1 = \lfloor (f_H - f_L)/B \rfloor \tag{19}$$

If using N carriers among N'_1, there will be $(N'_1 - N + 1)$ in total. Therefore, the absolute key amount can be calculated by using Eq. (15). The following equation is also available.

$$E_{a1} = 2\log_2 N + \log_2 (N'_1 - N + 1) \tag{20}$$

The second term of the equation is the increment of the absolute key amount in this situation. While synthesizing Eqs.(15), (19) and (20), the absolute key amount will be

$$E_{a1} = \min\{\lceil 2\log_2 N'_1 \rceil, \lceil 2\log_2 N + \log_2 (N'_1 - N + 1) \rceil\} \tag{21}$$

For the unequal-interval FH system, supposing the minimum interval of carriers is B', the total number of carriers that can be held in $[f_H, f_L]$ will increase to N'_2 from N. But it should satisfy the following restrictions:

$$f_H - f_L - B' \leqslant \sum_{j=1}^{N'_2} k_j \Delta f \leqslant f_H - f_L \tag{22}$$

The definitions of the parameters in this equation are the same as they were aforementioned. From Eq.(22), N'_2 is gotten as long as f_H, f_L and B' are given. Meanwhile, every element of the carrier set can also be gotten from Eq.(7) as

$$f_{c,j} = f_L + \sum_{j=1}^{N'_2} k_j \Delta f \tag{23}$$

Because B' is the minimum interval of the system, there should be $N < N'_2 < N'_1$ in most cases. If taking N in all N'_2 carriers, there will be $C^N_{N'_2}$ ways in total. However, when using the absolute key amount of FH to evaluate the difficulties of getting the practical carrier set, the absolute key amount is either

$$E_{a2} = N'_2 \log_2 N'_2 \tag{24}$$

or

$$E_{a2} = N'_1 \log_2 N'_1 - \log_2 C^N_{N'_2} \tag{25}$$

Synthesizing Eqs. (21) and (25), the absolute key amount in this situation should be

$$E_{a2} = \min\{[N'_2 \log_2 N'_2], [N'_1 \log_2 N'_1 - \log_2 C^N_{N'_2}]\} \tag{26}$$

When comparing Eqs.(21) to (26), it is clear that in overlap allowable FH systems, the absolute key amounts of equal-interval and unequal-interval systems will both be enhanced with the increment of the total number of carriers. But the increment of the latter one is far more than that of the former. More straightforward explanations will be given as follows.

For example, an FH communication system is working at 2 400 to 2 483.5 MHz ISM band, using 100 FH channels, and requiring a 200 kHz minimum interval. To compare the absolute key amounts between equal-interval and non unequal-interval systems, there is

$f_H - f_L = 83.5$ MHz, $N = 100$, $B' = 0.2$ MHz

For the equal-interval system, $N' = 417$. According to Eq.(26),

$E_{a1} = \min\{17.4, 21.6\}$ bits $= 17.4$ bits

For the non unequal-interval system, suppose $N'_2 = 0.6$ and $N'_1 \approx 250$. According to Eq.(26),

$E_{a2} = \min\{1\ 991.4, 3\ 629.5 - 238.5\}$ bits $=$ 1 991.4 bits

As another example, if an FH communication system is working at 5 725 to 5 850 MHz ISM, using 200 FH channels, and requiring a 200 kHz minimum interval. Also, we can compare the absolute key amounts between equal-interval and unequal-interval systems. From the above supposition,

$f_H - f_L = 125$ MHz, $N = 200$, $B' = 0.2$ MHz

For the equal-interval system, $N' = 625$. According to Eq.(21),

$E_{a1} = \min\{18.6, 24.0\}$ bits $= 18.6$ bits

For the non unequal-interval system, suppose $N'_2 = 0.6$ and $N'_1 = 375$. According to Eq.(26),

$E_{a2} = \min\{3\ 206.5, 5\ 804.8 - 560.4\}$ bits $=$ 3 206.5 bits

From the two examples above, it is obvious that

when the method of unequal-interval FH systems is adopted, its absolute key amount is greatly increased, especially in the spectrum overlap allowable systems. Since the total number of carriers is increased, the absolute key amounts of both equal-interval and unequal-interval FH systems are increased. But the increment of the latter is far larger than that of the former.

4 Conclusion

With the increasingly wide use of frequency hopping systems, people's demands for security and secrecy have become greater and greater. Based on the principles of information theory, definitions of relative and absolute key amounts of FH systems, equal-interval and unequal-interval FH systems are given firstly in this paper. Then the analysis of relative and absolute key amounts of equal-interval and unequal-interval FH systems shows that only if both of them are large enough can the FH system be cryptical and secure. And in today's epoch of highly developed computer science and integrated circuit design (IC), the absolute key amount has gradually become the key point in improving the security and secrecy of FH systems. Therefore, in this paper a novel method of unequal-interval FH systems is proposed. The ways to achieve the overlap unallowable system and overlap allowable system are presented respectively. And their performance in security is analyzed theoretically. From the examples, it is clear that adopting the unequal-interval system will increase its absolute key amount significantly, especially in overlap allowable FH systems, the absolute key amount is two orders larger than those of equal-interval FH systems.

References

[1] Bluetooth SIG. Bluetooth Technology Standard V1.1 [EB/OL]. http://www.bluetooth.com. 1999-12-10/2004-09-20.

[2] LAN/WAN Standards Committee of the IEEE Computer Society. IEEE 802.11 wireless LAN medium access control and physical layer specifications [EB/OL]. http://www.ieee.org. 1999-12-25/2004-09-20.

[3] Ye Zhihui, Shen Lianfeng, Song Tiecheng. Interference analysis and improvement of capacity reduction for FHSS networks in WPAN application environment [J]. *Journal of Southeast University (English Edition)*, **2003, 19**(3): 205-211.

[4] Fainberg M, Goodman D. Analysis of the interference between IEEE 802.11b and Bluetooth systems [A]. In: *IEEE VTS 54th*[C]. **New Jersey, 2002, 2**: 967-971.

[5] Andrew S, Park R, Buehrer M. Throughput performance of an FHMA system with variable rate coding [J]. *IEEE Transaction on Communications*, **1998, 46**(4): 521-532.

[6] Stranne A, Floren R, Edfors O, et al. FHSS networks in the presence of strongly interfering Bluetooth networks [A]. In: *Proceeding of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* [C]. **Lisbon, Portugal, 2002, 1**: 161-165.

[7] Sklar Bernard. *Digital communications fundamentals and applications*. 2nd ed. [M]. New Jersey: Prentice Hall PTR, 2001. 890-940.

[8] Cover Thomas M, Thomas Joy A. *Elements of information theory* [M]. New York: Wiley, 1991.

[9] Zhang J, Wong K M, Luo Z Q, et al. Blind adaptive FRESH filtering for signal extraction [J]. *IEEE Transaction on Signal Processing*, **1999, 47**(5): 1397-1402.

一种提高跳频系统密钥量的新方法

沈 斐 宋铁成 叶芝慧 刘 彤 夏玮玮

(东南大学移动通信国家重点实验室, 南京 210096)

摘要: 基于信息论原理, 提出了一种非等间隔跳频系统的方案, 针对不允许频谱重叠系统和允许频谱重叠系统, 分别给出了实现方法并对其安全性能进行了理论分析. 首先给出了跳频系统的绝对密钥量和相对密钥量、等间隔和非等间隔跳频系统等定义; 然后分析了等间隔和非等间隔跳频系统的绝对密钥量和相对密钥量, 从而看出在计算机技术和集成电路设计技术得到飞速发展的情况下, 跳频系统的绝对密钥量已变成制约其保密性和安全性的关键; 理论分析和实例计算可以看出, 采用非等间隔跳频后其绝对密钥量有大幅度提高, 特别是允许频谱重叠的系统, 比等间隔跳频系统提高了 2 个数量级以上.

关键词: 跳频系统; 密钥量; 信息安全; 非等间隔载频; 频移滤波器

中图分类号: TN914; TN925