A Combinatorial Framework for Frequency Hopping Multiple Access

Keith Martin, Siaw-Lynn Ng, Mwawi Nyirenda
{Keith.Martin, S.Ng, Mwawi.NyirendaKayuni.2011}@live.rhul.ac.uk
Information Security Group, Royal Holloway, University of London, UK

Abstract. In this paper we provide a combinatorial framework for analysing the performance of frequency hopping sequences in a multiple access system in the presence of a communication jammer. We examine the resilience of a scheme based on Latin squares which achieves maximum throughput and propose further schemes with the same throughput but better resilience. We also consider the parameters and trade-offs in the design of good frequency hopping multiple access schemes.

1 Introduction

Frequency hopping spread spectrum (FHSS) is a modulation technique that is widely used in Bluetooth, military and radar technologies [7]. A pair of communicating users follow a sequence that specifies the order of frequency channels for transmission or reception of data. It offers good narrowband interference suppression as well as the ability to place more systems in the same geographical area than other spread spectrum technologies. In frequency hopping multiple access (FHMA) users use frequency hopping sequences defined on the same set of frequency channels. However, *mutual interference* occurs when two or more transmitters use the same frequency channel simultaneously, resulting in signal loss. When interference comes from adversarial sources then we call it *jamming*. The adversary in this is context is called a *jammer*.

Background. Much research in the literature focuses on mitigating the problem of mutual interference. Many FH sequences are constructed using combinatorial designs and codes and are based on well-known bounds on Hamming correlation developed by Lempel and Greenberger in [5] and by Peng and Fan in [6]. For example, in [8], low rate Reed-Solomon codes are used to construct FH sequences and in [2], FH sequence sets meeting the Peng-Fan bounds were constructed using cyclotomic numbers, Reed-Solomon codes and cyclic difference matrices. The majority of the research for an FHMA is based on pairwise Hamming correlation. However, in an FHMA more than two users may transmit at a particular time. The inadequacy of the pairwise criterion was discussed in [10]. In this paper we will analyse the performance of an FH sequence in the presence of other *subsets* of FH sequences. All these research work do not consider the effect of a jammer on the constructed FH sequences.

On the other hand, [1,3] focus on the effect of a jammer only. In [3], FH sequences were constructed as a random walk on an expander graph, and [1] gave a construction using a pair of orthogonal Latin squares. In both constructions a jammer can eavesdrop and jam. However in both, the correlation properties of the constructed FH sequences are not considered.

Our contribution. We propose a combinatorial framework in which the effects of *both* mutual interference and jamming may be analysed and propose measurements for efficiency and resilience for an FHMA. Then we examine the resilience of the FH scheme in [1] which achieves maximum throughput. We provide two schemes also using Latin squares which are efficient and strongly resilient.

2 The model

System model. Let $\mathcal{F} = \{f_0, f_1, \ldots, f_{m-1}\}$ be a set of m available frequency channels called the *frequency library* where m is a positive integer.

Definition 1. *A sequence $X = (x_t)_{t=0}^{v-1}$ (or $X = (x_t)$ if there is no ambiguity) is called a frequency hopping sequence (FH sequence) of length v over $\mathcal{F}$ if $x_t \in \mathcal{F}$ for all $0 \leq t \leq v-1$.*

Definition 2. *A $(v, m, k)-$frequency hopping scheme ((v, m, k)-FHS)*[1]*, is a set $\mathcal{S} = \{X_g : 0 \leq g \leq k-1\}$ of size k where X_g is an FH sequence of length v over a frequency library $\mathcal{F}$ of size m.*

A set of n users $\mathcal{N} = \{N_i | 0 \leq i \leq n-1\}$ communicate pairwise using an FHMA with a given (v, m, k)-FHS $\mathcal{S}$. The sequences are used periodically. They wish to maximize their throughput in the presence of mutual interference and jamming. Each user selects[2] sending and receiving FH sequences from $\mathcal{S}$.

Attacker model. We assume the presence of a jammer J, which is not a legitimate user. It knows $\mathcal{N}$, $\mathcal{F}$ and $\mathcal{S}$ and has enough resources to eavesdrop on $\theta_1 m$ ($0 < \theta_1 < 1$) channels and jam on $\theta_2 m$ ($0 \leq \theta_2 < 1$) channels at each time slot. Its activity can be viewed as FH sequences $\mathcal{S}_J = \{S_g^J | S_g^J = (s_t^{J,g}), g = 0, \ldots, \theta_2 m - 1\}$, where S_g^J is an FH sequence of length v over $\mathcal{F}$. We call $\mathcal{S}_j$

[1] A (v, m, k)-FHS, $\mathcal{S}$, can be written in the language of codes. We may consider $\mathcal{S}$ as a set of k codewords of length v over an alphabet $\mathcal{F}$ of size m.

[2] Note that there are different algorithms for this: an FH sequence could simply be assigned by some central controlling user, or the users could have predistributed keys allowing them to choose an FH sequence.

the jamming sequences. We assume the jammer operates on the physical layer of the open systems interconnect model, therefore it sends noisy signals on a frequency channel(s) that interfere with the communication of legitimate users. We treat the jamming as an erasure. A jammer is successful if it reduces the transmission capacity of nodes by a significant proportion. Thus one of the goals of an (v, m, k)-FHS is to reduce the performance of a jammer.

3 Performance evaluation

The number of blocked frequency channels between a pair of FH sequences is given by the Hamming correlation, defined as follows:

Definition 3. *The Hamming correlation, $H_{X_g,X_h}(\tau)$, at relative time delay τ between a pair of FH sequences $X_g = (x_t^g)$ and $X_h = (x_t^h)$ of length v is defined as $H_{X_g,X_h}(\tau) = |\{x_t^g | x_t^g = x_{t+\tau}^h, 0 \leq \tau < v\}|$, where the addition of position indices is done modulo v.*

We assume that communication is synchronised and all users start $t = 0$ at the same time. Shifts of a sequence are treated as distinct sequences if needed. Therefore we only consider periodic cross-correlation of sequences in a (v, m, k)-FHS.

As mentioned earlier, in an FHMA where more than two users may transmit at the same time, the Hamming pairwise criterion which is widely used in literature is inadequate [10]. We thus introduce the Hamming group correlation, a parameter that measures the performance of an FH sequence in the presence of subsets of FH sequences.

Definition 4. *Let $\mathcal{S}$ be a (v, m, k)-FHS. Let $\mathcal{S}_\pi$ be a subset of $\mathcal{S}$ of size πn, $0 < \pi \leq 1$. Let $X_g \in \mathcal{S}$. The Hamming group correlation*[3]*, $G(X_g, S_\pi)$, between X_g and the FH sequences in $\mathcal{S}_\pi$ is the number of coordinates in X_g that contain the same symbols as the corresponding coordinates of some FH sequence in $\mathcal{S}_\pi$, $G(X_g, S_\pi) = |\{x_t^g | \exists X_h \in \mathcal{S}_\pi \text{ such that } x_t^h = x_t^g, t = 0, \ldots, v-1\}|$.*

Clearly, if $X_g \in \mathcal{S}_\pi$ then $G(X_g, \mathcal{S}_\pi) = v$. If $X_g \notin \mathcal{S}_\pi$ then $G(X_g, S_\pi)$ gives the number of time slots where X_g is blocked by the sequences in $\mathcal{S}_\pi$. We want to minimise G.

Now we can define throughput in the presence of mutual interference.

Definition 5. *Let $\mathcal{S}$ be an (v, m, k)-FHS. Let $\dot{\mathcal{S}} \subseteq \mathcal{S}$, $|\dot{\mathcal{S}}| = \delta n$, $0 \leq \delta \leq 1$, where n is the size of the network. Let $X_g \in \dot{\mathcal{S}}$ and $\mathcal{S}_\delta = \dot{\mathcal{S}} \backslash \{X_g\}$. The throughput of X_g is the rate of successful transmission in a session, in the presence of $\mathcal{S}_\delta$, given by, $\rho_\delta(X_g, \dot{\mathcal{S}}) = 1 - \frac{G(X_g, \mathcal{S}_\delta)}{v}$.*

[3] If (v, m, k)-FHS is a set of k codewords of length v over $\mathcal{F}$, $|\mathcal{F}| = m$, then $G(X_g, S_\pi)$ is the group distance as defined in [4].

Given a particular $\delta n-$subset $\dot{\mathcal{S}}$ of a (v,m,k)-FHS, we can define the average throughput, $\bar{\rho}_\delta(\dot{\mathcal{S}}) = \frac{1}{\delta n}\sum_{X_i \in \dot{\mathcal{S}}} \rho_\delta(X_i, \dot{\mathcal{S}})$ and the worst case[4] throughput, $\hat{\rho}_\delta(\dot{\mathcal{S}}) = \min_{X_i \in \dot{\mathcal{S}}}\{\rho_\delta(X_i, \dot{\mathcal{S}})\}$. Clearly $0 \leq \bar{\rho}_\delta, \hat{\rho}_\delta \leq 1$ and in Section 4 we examine schemes with $\delta = 1$ and $\bar{\rho}_1 = 1$

We may also define the throughput in the presence of both mutual interference and a jammer.

Definition 6. *Let $\mathcal{S}$ be an (v,m,k)-FHS. Let $\dot{\mathcal{S}} \subseteq \mathcal{S}$, $|\dot{\mathcal{S}}| = \delta n$, $0 \leq \delta \leq 1$, where n is the size of the network. Let $X_g \in \dot{\mathcal{S}}$ and $\mathcal{S}_\delta = \dot{\mathcal{S}} \backslash \{X_g\}$. The throughput of X_g in the presence of $\mathcal{S}_J$, $|\mathcal{S}_J| = \theta_2 m = \theta n$ and $\mathcal{S}_\delta$ is the rate of successful transmission in a session, $0 \leq \rho_{\delta+\theta}(X_g, \dot{\mathcal{S}} \cup \mathcal{S}_J) = 1 - \frac{G(X_g, \mathcal{S}_\delta \cup \mathcal{S}_J)}{v}$.*

Definition 7. *A (v,m,k)-FHS, $\mathcal{S}$ is said to be (γ,ϵ)-**strongly resilient** against a $(\gamma,\epsilon,\theta_1,\theta_2)$-jammer that listens to at most $\theta_1 m$ channels at each time, for γv time slots and jams at most $\theta_2 m$ channels at a time, if it can reduce the worst case throughput $\hat{\rho}_\delta(\dot{\mathcal{S}})$ to not less than $\epsilon\hat{\rho}_\delta(\dot{\mathcal{S}})$.*

If a jammer is capable of jamming one channel at each time slot, then it is successful with probability $\frac{1}{m}$. Thus any scheme can be at most $(1, 1-\frac{1}{m})$-strongly resilient. In the next sections we consider a scheme that is not $(\frac{1}{v}, 0)$-strongly resilient and two schemes which are $(1, 1-\frac{1}{m})$-strongly resilient.

4 Frequency hopping schemes without mutual interference

4.1 The Bag-Ruj-Roy (BRR) scheme [1]

Notation. Let L be a Latin square over $\mathbb{Z}_n$ and $x \in \mathbb{Z}_n$. We write $L + x$ to denote the $n \times n$ array where each entry a_{ij} of L is replaced by $a_{ij} + x$ mod n. It is easy to see that $L + x$ is a Latin square if L is. If L_1 and L_2 are two orthogonal $n \times n$ Latin squares defined on $\mathbb{Z}_n$ and $x, y \in \mathbb{Z}_n$ then $L_1 + x$ mod n and $L_2 + y$ mod n are orthogonal Latin squares.

The Bag-Ruj-Roy (BRR) [1] scheme is as follows. The network $\mathcal{N}$ has n users $\{N_0, \ldots, N_{n-1}\}$ and the frequency library has size n with $\mathcal{F} = \mathbb{Z}_n$. The frequency hopping scheme is an (n,n,n)-FHS defined by two orthogonal Latin squares $L_1 = [\alpha_{ij}]_{n\times n}$ and $L_2 = [\beta_{ij}]_{n\times n}$. All users generate the same session keys x, y as follows $x = F_1(K,s)$ and $y = F_2(K,s)$ where F_1 and F_2 are pseudorandom functions that takes inputs K, s, the long term key shared by all users and the session number respectively.

The jammer knows $\mathcal{N}$, $\mathcal{F}$ and $\mathcal{S}$. We assume it can eavesdrop on one channel and jam on one channel, so $\theta_1 = \theta_2 = \frac{1}{n}$.

[4] Considering (v,m,k)-FHS as a code, then a (v,m,k)-FHS with worst case throughput $\hat{\rho}_\delta(\dot{\mathcal{S}}) > \alpha$ is precisely a $(\delta n, \alpha)$-cover free code [9] studied in the context of traceability codes.

At each session, the sending FH sequences are derived from $S_g^* = \{(\alpha_{gj} + x, \beta_{gj} + y, j) | 0 \leq j \leq n-1\}$ where $\alpha_{gj} \in L_1$ and $\beta_{gj} \in L_2$. User N_g transmit to user N_j on frequency channel $\alpha_{gj} + x$ at time slot $\beta_{gj} + y$.

Note that $L_1 + x$ and $L_2 + y$ are orthogonal Latin squares and all the frequency channels at each time slot are distinct. This implies that there is no mutual interference at each time slot for all $\mathcal{S}$. Hence $\bar{\rho}_\delta(\mathcal{S}) = 1$. However, it can easily be shown that the (n, n, n)-FHS is not $(\frac{1}{n}, 0)$-strongly resilient.

Attack. Suppose the jammer eavesdrop on frequency f_e at time t where user N_g was transmit to user N_h. Thus the jammer discover one hop element, $(f_e, t, j) = (\alpha_{gh} + x, \beta_{gh} + y, h)$. Then the jammer can retrieve x and y, by solving the linear equations $\alpha_{gh} + x$ and $\beta_{gh} + y$. It can then derive the FH sequence of any user. The BRR scheme is thus not $(\frac{1}{n}, 0)$-strongly resilient.

4.2 Strongly Resilient Bag-Ruj-Roy (sR-BRR) scheme

The BRR scheme can be made into a strongly resilient scheme as follows. Instead of session keys, all users generate new keys for each frequency slot called *slot keys*: $x_t = F_3(K, s, t)$ and $y_t = F_4(K, s, t)$ where F_3 and F_4 are pseudorandom functions. A user N_g looks up row g in L_2 to find the entry $\beta_{gj} = y_t$. Let α_{gj} be the corresponding value of β_{gj} in L_1. Then the new frequency hop is given by $\alpha_{gj} + x_t$. Essentially this scheme generates a new BRR scheme for each time slot.

The scheme has the same throughput as the BRR scheme, hence $\rho_1 = 1$. Since the slot keys are updated at every slot, the jammer cannot derive any FH sequence as long as the pseudorandom number generator is secure. Hence the sR-BRR is $(1, 1 - \frac{1}{m})$-strongly resilient.

4.3 Strongly resilient Latin square (sR-LS) scheme

Let $L = [\alpha_{ij}]_{n \times n}$ be a Latin square of order n defined on $\mathbb{Z}_n$. An FH sequence is derived as $\acute{S}_g = (s_t^g | s_t^g = \alpha_{gt} + x_t)$ where $\alpha_{gt} \in L$, $x_t = F_3(K, s, t)$, F_3 a pseudorandom function, K a long time shared key among all users, s the session number and t the time slot.

The sR-LS only uses one Latin square. There is no mutual interference among all transmitters at each time slots because all frequency channels $\alpha_{gt} + x_t, 0 \leq g \leq n-1$ are distinct. Further, the scheme is $(1, 1-\frac{1}{m})$-strongly resilient.

5 Conclusion

In this paper, we presented a new framework for analysing the performance of FHMA systems in the presence of both mutual interference and a jammer. Further, we have shown that Latin squares can easily be used for strongly resilient schemes at the expense of computation. It will be interesting to study further trade-offs between the parameters of throughput, computation and resilience and it will be interesting to see if these schemes can be made scalable.

References

[1] S. Bag, S. Ruj and B. Roy, Jamming Resistant Schemes for Wireless Communication: A Combinatorial Approach, *Information Systems Security*, Springer Lecture Notes in Computer Science, **8303**, 43–62, 2013.

[2] C. Ding , R. Fuji-Hara , Y. Fujiwara , M. Jimbo and M. Mishima, Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions, *Information Theory*, IEEE Transactions, **55**, 3297–3304, 2009.

[3] Y. Emek and R. Wattenhofer, Frequency Hopping against a Powerful Adversary, *Distributed Computing*, Springer Lecture Notes in Computer Science, **8205**, 329–343, 2013.

[4] H. Jin and M. Blaum, Combinatorial Properties for Traceability Codes Using Error Correcting Codes, *Information Theory*, IEEE Transactions, **53**, 804–808 2007.

[5] A. Lempel and H. Greenberger, Families of Sequences with Optimal Hamming Correlation Properties, *Information Theory*, IEEE Transactions, **20**, 90-94, 1974.

[6] D. Peng and P. Fan, Lower Bounds on the Hamming Auto- and Cross-Correlations of Frequency Hopping Sequences, *Information Theory*, IEEE Transactions, **50**, 2149-2154, 2004.

[7] J. Proakis, Digital Communications, *McGraw-Hill*, 1995.

[8] D. V. Sarwate, Reed-Solomon Codes and the Design of Sequences for Spread Spectrum Multiple Access Communications, *Reed-Solomon Codes and their Applications*, IEEE Press, edited by S. B. Wicker and V. K. Bhargava, 175–204, 1994.

[9] J. N. Staddon and D. R. Stinson and R. Wei, Combinatorial properties of frameproof and traceability codes, *IEEE Trans. Inf. Theory*, **47(3)**, 1042-1049, 2001.

[10] Q. Wang and M. Wang, On Frequency-Hop Multiple Access Sequence, *1st International Conference on Universal Personal Communications*, **17**, 0177–0181, 1992.