Anti-Jamming Frequency Hopping Techniques for Secure Multicast Communications

Mohammad J. Abdel Rahman and Marwan Krunz
Department of Electrical and Computer Engineering, University of Arizona
Tucson, AZ 85721, USA
{mjabdelrahman, krunz}@email.arizona.edu

ABSTRACT

We address the problem of jamming mitigation of multicast communications in multi-channel ad hoc networks. Specifically, we develop two frequency hopping (FH) techniques for establishing multicast communications. These techniques, denoted by KFH and CFH, address the two following problems. First, establishing multicast communications in the presence of a control-channel jamming attack. Second, redistributing the secret keys (i.e., PN codes) once the current keys have been exposed by a smart eavesdropping jammer. Our techniques are distributed, do not incur any additional message exchange overhead, work in the absence of node synchronization, and maintain the multicast group consistency.

1. INTRODUCTION

Wireless communications are vulnerable to intentional interference attacks, typically referred to as jamming. Conventional anti-jamming techniques rely extensively on spread spectrum (SS) communications, including frequency hopping spread spectrum (FHSS).

We consider two types of jamming attacks: control-channel denial of service (DoS) attacks, and the smart eavesdropper jamming attack. The operation of a wireless network relies extensively on exchanging messages over a control channel. The network performance can be severely degraded if a jammer lunches a DoS attack on such a channel. In the presence of a smart eavesdropping jammer, FH sequences may be (eventually) partially figured out by the eavesdropper, who may attempt to persistently target certain frequencies in certain time slots.

In this work, we propose two FH techniques that can establish multicast communications in the presence of a control-channel DoS attack and/or smart eavesdropper attack. Our techniques have four important features: (i) They are fully distributed, (ii) they do not incur any additional message exchange overhead, (iii) they can establish multicast links in the absence of node synchronization, and (iv) in contrast to [2], they maintain the multicast group consistency, where at any time instant all nodes have consistent keys.

Our FH algorithms, denoted by KFH and CFH, rely on special types of *quorum systems* that satisfy the *rotation k-closure property*. KFH is based on the *uniform k-arbiter quorum system* and CFH is based on the *Chinese remainder theorem (CRT) quorum system*. The rotation k-closure property enables these FH techniques to operate in the absence of node synchronization.

2. QUORUM SYSTEMS

This section briefly introduces quorum systems and explains the rotation k-closure property.

DEFINITION 1. *Given a set $Z_n = \{0, \ldots, n-1\}$, a quorum system Q under Z_n is a collection of non-empty subsets of Z_n, each called a quorum, such that $\forall G, H \in Q : G \cap H \neq \emptyset$.*

DEFINITION 2. *A quorum system Q under Z_n is said to satisfy the rotation k-closure property if $\forall G_1, G_2, \ldots, G_k \in Q$ and $\forall i_1, i_2, \ldots, i_k \in Z_n$, $\bigcap_{j=1}^{k} rotate(G_j, i_j) \neq \emptyset$.*

3. KFH ALGORITHM

The KFH algorithm uses the uniform k-arbiter quorum system, which is known [1] to exhibit the rotation $(k+1)$-closure property.

DEFINITION 3. *A k-arbiter quorum system Q under Z_n is a collection of quorums such that $\bigcap_{i=1}^{k+1} G_i \neq \emptyset, \forall G_1, G_2, \ldots, G_{k+1} \in Q$.*

DEFINITION 4. *A quorum system Q under Z_n that satisfies $Q = \{G \subseteq Z_n : |G| = (\lfloor kn/(k+1) \rfloor + 1)\}$ is called a uniform k-arbiter quorum system.*

In KFH (similarly CFH), each FH sequence consists of several time frames. Each frame consists of a block of consecutive time-frequency hops. We explain the KFH algorithm using the following example. Suppose that the number of nodes is 3, the frame length (denoted by n) is 4, and the set of channels is $\{f_1, f_2, \ldots, f_L\}$.

STEP 1: Construct a universal set $Z_4 = \{0, 1, 2, 3\}$.

STEP 2: Construct a uniform 2-arbiter quorum system Q under Z_4.

STEP 3: Construct an FH sequence $\boldsymbol{w}$ using the following procedure:

- Select a quorum G from the quorum system Q.
- Assign frequency h to the FH slots that correspond to G, and assign a random frequency h_x to the other slots, where h and $h_x \in \{f_1, f_2, \ldots, f_L\}$.
- Repeat the above procedure for the other frames.

STEP 4: Repeat Step 3 to construct the other FH sequences.

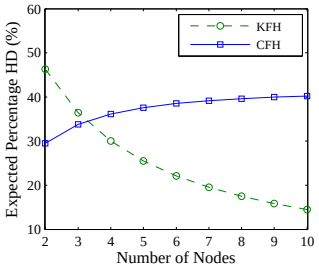

Figure 1: $\mathcal{D}$ for KFH and CFH ($L = 6$).

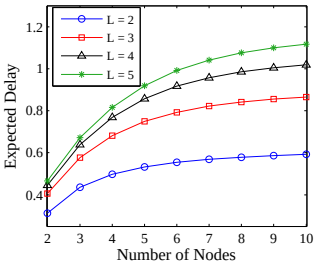

Figure 2: Expected delay for KFH.

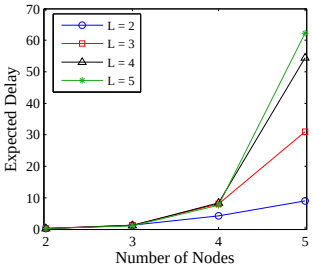

Figure 3: Expected delay for CFH.

4. CFH ALGORITHM

The CFH algorithm uses the Chinese remainder theorem (CRT) quorum system, which exhibits the rotation k-closure property. The CRT is formally described as follows.

THEOREM 1. *Let $p_1, \ldots, p_k$ be k positive integers that are pairwise relatively prime, i.e., $gcd(p_i, p_j) = 1, \forall i, j \in \{1, \ldots, k\}$, where $gcd(p_i, p_j)$ is the greatest common divisor of p_i and p_j. Let $y = p_1 p_2 \ldots p_k$ and let $z_1, \ldots, z_k$ be k integers, where $z_i < p_i, \forall i \in \{1, \ldots, k\}$. Then, $\exists$ a solution I for the following system of simultaneous congruences*:

$$z_1 \pmod{p_1} \equiv z_2 \pmod{p_2} \equiv \ldots \equiv z_k \pmod{p_k}.$$

Furthermore, any two solutions I and I' to the above system are congruent modulo y, i.e., $I' \equiv I \pmod{y}$. That is, there exists exactly one solution I between 0 and $y - 1$.

Using Theorem 1, we can construct quorum systems that satisfy the rotation k-closure property.

THEOREM 2: *Let $p_1, \ldots, p_k$ be k positive integers that are pairwise relatively prime, and let $y = p_1 \ldots p_k$. The CRT quorum system $Q = \{G_i : G_i = \{p_i c_i : c_i \in \{0, \ldots, y/p_i - 1\}\}, \forall i \in \{1, \ldots, k\}\}$ under Z_y satisfies the rotation k-closure property.*

The CFH algorithm for generating k asynchronous multicast FH sequences is the same as the KFH algorithm, with two differences. First, CFH uses the CRT quorum systems instead of the uniform k-arbiter quorum system. Second, the frame length is equal to $y = p_1 p_2 \ldots p_k$.

5. PERFORMANCE EVALUATION

5.1 Expected Percentage Hamming Distance (HD)

The expected percentage HD for two FH sequences $\boldsymbol{x} = (x_1 x_2 \ldots x_n)$ and $\boldsymbol{y} = (y_1 y_2 \ldots y_n)$, denoted by $\mathcal{D}^{(\boldsymbol{x},\boldsymbol{y})}$, is defined as $\mathcal{D}^{(\boldsymbol{x},\boldsymbol{y})} \stackrel{\text{def}}{=} E[D^{(\boldsymbol{x},\boldsymbol{y})}] = E[\left(\sum_{i=1}^{n} \mathbf{1}_{\{x_i \neq y_i\}}\right)/n]$, where $\mathbf{1}_{\{\cdot\}}$ is the indicator function. For simplicity, we drop the superscript in $\mathcal{D}^{(\boldsymbol{x},\boldsymbol{y})}$. In KFH, $\mathcal{D}$ is the same for all pairs of FH sequences, whereas in CFH they are different for different pairs. Thus, for CFH, we compute the expected value over all pairs of FH sequences.

Let $\mathcal{D}_{KFH}$ and $\mathcal{D}_{CFH}$ denote the value of $\mathcal{D}$ for the KFH and CFH algorithms, respectively. Then,

$$\mathcal{D}_{KFH} = \mu_1 \frac{(n - \lfloor \frac{kn}{k+1} \rfloor)\mu_3}{n} + (1 - \mu_1)\frac{(n - \lfloor \frac{kn}{k+1} \rfloor - 1)\mu_3}{n}$$

where $\mu_1 = \frac{\mu_2 - 1}{\mu_2}, \mu_2 = \binom{n}{\lfloor \frac{kn}{k+1} \rfloor + 1}$, and $\mu_3 = \frac{L-1}{L}$.

$$\mathcal{D}_{\text{CFH}} = \frac{L-1}{2k^2 nL} \sum_{i=1}^{k} \sum_{j=1}^{k} \left(n - \frac{n}{x_i x_j}\right).$$

Figure 1 depicts $\mathcal{D}$ vs. the number of nodes for the KFH and CFH algorithms when the number of channels $L = 6$. As the number of nodes increases, $\mathcal{D}_{CFH}$ increases whereas $\mathcal{D}_{KFH}$ decreases.

5.2 Expected Delay

The expected delay is defined as the expected time until the multicast link is established. Let $\mathcal{T}_{\text{KFH}}$ and $\mathcal{T}_{\text{CFH}}$ denote the expected delay for the KFH and CFH algorithms, respectively, where the expectation is taken over all possible random assignments. Then,

$$\mathcal{T}_{\text{KFH}} = \sum_{i=1}^{n-1} i \prod_{j=0}^{i-1}(1 - \beta(\alpha_j))\beta(\alpha_i)$$

where

$$\beta(\alpha_j) = \sum_{i=0}^{k} \binom{k+1}{i} \alpha_j^{k+1-i} \left(\frac{1-\alpha_j}{L}\right)^i + (1-\alpha_j)^{k+1}\left(\frac{1}{L}\right)^k$$

and $\alpha_i = \frac{\lfloor \frac{kn}{k+1} \rfloor - i + 2}{n} + \frac{\lfloor \frac{kn}{k+1} \rfloor - i + 3}{n-i+1}\frac{i-1}{n}$. Furthermore,

$$\mathcal{T}_{\text{CFH}} = \sum_{i=1}^{n-1} i(1-\varphi)^{i-1}\varphi,$$

where

$$\varphi = \sum_{i=0}^{k-1} \sum_{\substack{\forall \{s_1, s_2, \ldots, s_{k-i}\} \\ \in \{x_1, x_2, \ldots, x_k\}}} \left[\frac{1}{s_1 s_2 \ldots s_{k-i}} \left(\frac{1}{L}\right)^i \prod_{j=k-i+1}^{k}\left(1 - \frac{1}{s_j}\right)\right] + \left(\frac{1}{L}\right)^{k-1} \prod_{l=0}^{k-1}\left(1 - \frac{1}{s_l}\right)$$

k equals to the number of nodes minus one for $\mathcal{T}_{\text{KFH}}$, and the number of nodes for $\mathcal{T}_{\text{CFH}}$. Figures 2 and 3 show the expected delay for KFH and CFH, respectively. For both KFH and CFH, the expected delay increases with L and the number of nodes.

6. CONCLUSIONS

We proposed two FH algorithms, called KFH and CFH, for establishing multicast communications in the presence of a control-channel DoS attack and/or smart eavesdropper attack. We showed that KFH is faster than CFH, but CFH has better HD than KFH.

7. REFERENCES

[1] Y.-C. Kuo. Quorum-based power-saving multicast protocols in the asynchronous ad-hoc network. *Computer Networks*, 54:1911–1922, 2010.

[2] S. Liu, L. Lazos, and M. Krunz. Thwarting inside jamming attacks on wireless broadcast communications. In *Proc. of the ACM WiSec Conf.*, 2011.