Thwarting Control-Channel Jamming Attacks from Inside Jammers

Sisi Liu, *Student Member, IEEE,* Loukas Lazos, *Member, IEEE,* and Marwan Krunz, *Fellow, IEEE*
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ 85721
E-mail:{sisimm, llazos, krunz}@ece.arizona.edu

APPENDIX 1

*P*roposition 1: For two random and independently generated sequences m_j and m_ℓ, defined over an alphabet $\mathcal{A} = \{1, \ldots, K\}$, the expected Hamming distance $\mathrm{E}[d(m_j, m_\ell)]$ as a function of the sequence length X is given by

$$\mathrm{E}[d(s_j, s_\ell)] = \frac{K-1}{K}X. \tag{1}$$

Proof: The proof is a direct consequence of the randomness and independence assumptions. Based on the sequence generation process outlined in Section 4.1, $\Pr[m_j(i) = k] = \frac{1}{K},\ \forall i$. Since the two sequences m_j and m_ℓ are assumed to be independent and random, they differ at slot i with probability

$$\Pr[m_j(i) \neq m_\ell(i)] = \frac{K-1}{K}. \tag{2}$$

The expected Hamming distance between two sequences of length X is equal to the expected number of successes in X such Bernoulli trials, i.e., $E[d(m_j, m_\ell)]= \frac{K-1}{K}X$. □

APPENDIX 2

*P*roposition 2: Consider two random and independently generated sequences m_j and m_ℓ that are defined over an alphabet $\mathcal{A} = \{1, \ldots, K\}$. Suppose that the sequences are adjusted to m'_j and m'_ℓ, respectively, according to the process outlined in Section 4.2. The expected Hamming distance $E[d(m'_j, m'_\ell)]$ as a function of the length X of the sequences is

$$\begin{aligned}\mathrm{E}[d(m'_j, m'_\ell)] \;\;=\;\; & \left(1 - (K(i) - y_K)\cdot\left(\frac{x_K}{K}\right)^2 \right.\\ & \left. -y_K \cdot \left(\frac{x_K+1}{K}\right)^2\right)\cdot X \end{aligned} \tag{3}$$

where $x_K \triangleq \lfloor \frac{K}{K(i)} \rfloor$ and $y_K \triangleq [K \pmod{K(i)}]$.

Proof: According to Step 2 in Section 4.2, the hopping sequences are modified by a modulo $K(i)$ operation. The number of indexes of the original sequence that map to the same index in the modified sequence depends on the quotient of the division of K by $K(i)$, given by $x_K = \lfloor \frac{K}{K(i)} \rfloor$, and the remainder, given by $y_K = [K \pmod{K(i)}]$. In particular, for a modified sequence m'_j, it follows from elementary modulo arithmetic that

$$\Pr[m'_j(i) = w] = \begin{cases} \frac{x_K+1}{K}, & \text{if } 1 \leq w \leq y_k,\ y_k > 0. \\ \frac{x_K}{K}, & \text{if } y_k + 1 \leq w \leq K(i). \end{cases} \tag{4}$$

Let $\mathcal{M}$ be the event that two modified sequences m'_j and m'_ℓ match at slot i. Based on (4), we have

$$\Pr[\mathcal{M}] = \sum_{w=1}^{K(i)} \Pr[m'_j(i) = w, m'_\ell(i) = w] \tag{5a}$$

$$= \sum_{w=1}^{K(i)} \Pr[m'_j(i) = w] \Pr[m'_\ell(i) = w] \tag{5b}$$

$$= \sum_{w=1}^{y_k} \left(\frac{x_K+1}{K}\right)^2 + \sum_{y_K+1}^{K(i)} \left(\frac{x_K}{K}\right)^2 \tag{5c}$$

$$= y_K \cdot \left(\frac{x_K+1}{K}\right)^2 + \left(K(t_1) - y_K\right) \cdot \left(\frac{x_K}{K}\right)^2. \tag{5d}$$

Equation (5b) is due to the independence in the generation of the original sequences m_j and m_ℓ. Equation (5c) is due to the probability distribution in (4) and Equation (5d) follows from the simplification of the sum. Given $\Pr[\mathcal{M}]$, it is easy to see that the expected Hamming distance for two sequences of length X is given by (3). □

APPENDIX 3

*P*roposition 5: The optimal strategy of an external jammer is to continuously jam the channel that is most frequently visited by cluster nodes.

Proof: Let c_{jam} denote the subsequence of m_{jam} corresponding to the locations of control channel slots; i.e., $c_{jam} = \{m_{jam}(i) : i \in v\}$ (v denotes the random slot position vector). Let also $\mathcal{P} = \{p_1, p_2, \ldots, p_K\}$ and $\mathcal{Q} = \{q_1, q_2, \ldots, q_K\}$ denote the probability distribution functions from which values $c(i)$ and $c_{jam}(i)$ are drawn, respectively. $\mathcal{Q}$ is optimal when the expected Hamming distance $\mathrm{E}\left[d(c, c_{jam})\right]$ is minimized, i.e., the jammer is able to overlap with c in the maximum number of slots. Suppose that $\pi = \{\pi(1), \ldots, \pi(k)\}$ is a permutation of the set of channels $\{1, \ldots, K\}$ such that $p_{\pi(1)} \geq \ldots \geq p_{\pi(K)}$. That is, the discrete probabilities of $\Pr[c(i) = k]$ are arranged in descending order. The probability that c and c_{jam} overlap at index i (which corresponds to slot $v(i)$) is

$$\begin{aligned} \Pr[c(i) = c_{jam}(i)] &= \sum_{j=1}^{K} \Pr[c(i) = \pi(j), c_{jam}(i) = \pi(j)] \\ &= \sum_{j=1}^{K} p_{\pi(j)} q_{\pi(j)} \end{aligned} \quad (6)$$

For a sequence of length X, the expected Hamming distance between c and c_{jam} is $\mathrm{E}[d(c, c_{jam})] = (1 - \Pr[c(i) = c_{jam}(i)])X$ (overlapping in two different slots are independent events). Hence, the expected Hamming distance is minimized when (6) is maximized.

Maximization of (6) can be shown as follows. Consider two distributions $\mathcal{P} = \{p_1, p_2, \ldots, p_K\}$ and $\mathcal{Q} = \{q_1, q_2, \ldots q_K\}$, and also consider two cases for the distribution $\mathcal{Q}$: $\{q_{\pi(1)}, q_{\pi(2)}, \ldots, q_{\pi(K)}\} = \{1, 0, \ldots, 0\}$ and $\{q'_{\pi(1)}, q'_{\pi(2)}, \ldots q'_{\pi(K)}\}$ with $q'_{\pi(1)} < 1$. Let $S = \sum_{j=1}^{K} p_{\pi(j)} q_{\pi(j)}$ and $S' = \sum_{j=1}^{K} p_{\pi(j)} q'_{\pi(j)}$. Then,

$$\begin{aligned} S' - S &= \sum_{j=1}^{K} p_{\pi(j)} q'_{\pi(j)} - \sum_{j=1}^{K} p_{\pi(j)} q_{\pi(j)} \\ &= \sum_{j=1}^{K} p_{\pi(j)} q'_{\pi(j)} - p_{\pi(1)} \cdot q_{\pi(1)} \\ &\leq \sum_{j=1}^{K} p_{\pi(1)} q'_{\pi(j)} - p_{\pi(1)} \\ &= p_{\pi(1)} \sum_{j=1}^{K} q'_j - p_{\pi(1)} \\ &= 0. \end{aligned}$$

Hence, $\sum_{j=1}^{K} p_{\pi(j)} q_{\pi(j)}$ is maximized when the distribution $\{q_{\pi(1)}, q_{\pi(2)}, \ldots q_{\pi(K)}\} = \{1, 0, \ldots, 0\}$. □

APPENDIX 4

*P*roposition 6: In static spectrum networks, the expected evasion delay $\mathrm{E}[D]$ for re-establishing the control channel when no node has been compromised is

$$\mathrm{E}[D] = \frac{K}{K-1} \cdot \frac{L+M}{M}. \quad (7)$$

Proof: $\mathrm{E}[D]$ is equal to the expected number of required slots $\mathcal{N}$ before the control-channel slot occurs for the first time, times the number of tries $\mathcal{R}$ needed to evade jamming. Thus,

$$\mathrm{E}[D] = \mathrm{E}[\mathcal{R}\mathcal{N}] = \mathrm{E}[\mathcal{R}]\mathrm{E}[\mathcal{N}]. \quad (8)$$

Note that $\mathcal{R}$ and $\mathcal{N}$ are independent random variables. The probability of evading jamming for random hopping sequences, assuming an optimal jamming strategy, is equal to $\frac{K-1}{K}$. Thus, $\mathrm{E}[\mathcal{R}] = \frac{K}{K-1}$. By construction, slot i is a control-channel slot with probability $\frac{M}{L+M}$. Therefore, the first re-occurrence of the control channel follows a geometric distribution with parameter $\frac{M}{L+M}$, and $\mathrm{E}[\mathcal{N}] = \frac{L+M}{M}$. Substituting $\mathrm{E}[\mathcal{R}]$ and $\mathrm{E}[\mathcal{N}]$ into (8) completes the proof. □

APPENDIX 5

*P*roposition 7: The expected delay until the new CH assigns new hopping sequences to $n-1$ cluster nodes (excluding the compromised CH) is

$$\mathrm{E}[D_2] = \frac{K^2}{K-1}(n-1)X_c. \quad (9)$$

Proof: Once the CH is considered compromised, all cluster nodes hop according to self-generated random sequences. Let m_{CH} denote the hopping sequence of the new CH. The CH succeeds in communicating with node n_j at slot i if $m_{CH}(i) = m_j(i)$ and $m_{CH}(i) \neq m_{jam}(i)$. Given that the sequences m_j and m_{CH} are random,

$$\Pr[m_j = m_{CH}, m_j \neq m_{jam}] = \frac{1}{K} \frac{K-1}{K} = \frac{K-1}{K^2}. \quad (10)$$

The number of slots until the first success is geometrically distributed with mean of $\frac{K^2}{K-1}$. The CH has to repeat the same process for all $n-1$ cluster nodes (the compromised CH is excluded from the hopping sequence update process). Assuming that X_c time slots are needed for the assignment of the new sequence, the expected delay $E[D_2]$ until all cluster nodes have received a new hopping sequence is equal to $\frac{K^2}{K-1}(n-1)X_c$. □