Time-Delayed Broadcasting for Defeating 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: The FH sequences constructed by Algorithm 1 are uniformly distributed.

Proof: Let $h_j = \{x_1, x_2, \ldots\}$ denote a FH sequence constructed by Algorithm 1 for a node v_j, where x_i is the frequency band assigned to v_j during slot i. Let x_i conform to a distribution X. We will show that in Algorithm 1, X is the uniform distribution. The x_i is defined by the permutation $\pi \in P_K$ randomly selected for each slot i, where P_K denotes all possible permutations of the available frequency band set $\mathcal{C}$. Selection of π is done with replacement and is independent of selections in prior slots. At each slot i, v_j is assigned to rendezvous on frequency band $\pi(m)$, where $\pi(m)$ denotes the m^{th} element of the permutation π. Hence,

$$\begin{aligned} \Pr\left[x_i = f_\ell\right] &= \sum_m \Pr\left[v_j \text{ assigned to } p(m)\right] \Pr\left[p(m) = f_\ell\right] \\ &= \sum_k \frac{1}{K} \frac{(K-1)!}{K!} \\ &= \frac{1}{K}. \end{aligned} \tag{1}$$

In (1), v_j is assigned to any of the K elements of π with equal probability since the order of the rendezvous pairs within a 1-factor is random (the pair order in a 1-factor can be arbitrarily shuffled). Moreover, there are $(K-1)!$ permutations out of the total $K!$ permutations in P_K for which $\pi(m) = f_\ell$. As a result, the value x_i conforms to the uniform distribution and the FH sequence h_j is uniformly distributed. □

We emphasize here that FH sequences assigned to each node are random in terms of the probability of occurrence of a particular frequency band at any given slot i. However, the FH sequences assigned to two nodes are not independent. This is because at each slot, the frequency bands assigned to each pair of nodes forms a permutation. Knowing the assigned FH sequence of one node immediately reduces the uncertainty for the FH sequences of other nodes. This fact is exploited in the design of the optimal jamming strategy when FH sequences are compromised. The adversary uses the compromised FH sequences to reduce the space of possible frequency bands assigned to uncompromised pairs of nodes.

APPENDIX 2

*P*roposition 2: The minimum number of FH schedule changes for existing broadcast group members when migrating from $\mathcal{F}_{2n}$ to $\mathcal{F}_{2n+2}$ due to member addition is $(8n-4)$. This minimum is achieved when $(2n-2)$ pairs are split and four pairs are deferred.

Proof: Let two nodes v_{2n+1} and v_{2n+2} be added to a broadcast group of size $2n$. In the extension of F_{2n} to F_{2n+2} schedule changes for existing nodes can occur due to (a) a rendezvous between a newly added node and an existing one and (b) rescheduling of an node pair between existing nodes from $F_i \in \mathcal{F}_{2n}$ to $F_j \in F_{2n+2}, i \neq j$. We compute the minimum number of schedule changes for each type.

(a) Changes due to rendezvous between a newly added node and an existing one: In $\mathcal{F}_{2n+2}$, nodes v_{2n+1} and v_{2n+2} must rendezvous with each of the existing nodes $\{v_1, \ldots, v_n\}$ (in order to form a proper 1-factorization). Hence, a total of $4n$ new node pairs formed by one existing node and one newly added node must be scheduled. For these pairs, existing nodes incur one schedule change. Therefore, the least number of schedule changes due to the formation of new node pairs is $4n$ (Node that more than $4n$ schedule changes may be required if the existing nodes that meet with the newly added nodes on a given 1-factor in $\mathcal{F}_{2n+2}$ do not form a split pair on the same 1-factor in $\mathcal{F}_{2n}$).

(b) Rescheduling of existing node pairs: 1-factorization $\mathcal{F}_{2n+2}$ has two more 1-factors compared with F_{2n}. Moreover, every 1-factor of F_{2n+2} has $(n+1)$ pairs. The two extra 1-factors of $\mathcal{F}_{2n+2}$, denoted by F_{2n-1} and F_{2n}, accommodate in total $2(n+1)$ node pairs. If node pair (v_{2n+1}, v_{2n+2}) is not part of either F_{2n-1} or F_{2n}, these two 1-factors must accommodate four deferred pairs. This is because by the 1-factorization definition, nodes v_{2n+1} and v_{2n+2} rendezvous with two existing nodes at every 1-factor that does not contain pair (v_{2n+1}, v_{2n+2}). Consequently, the remaining $(2n-2)$ node pairs in F_{2n-1} and F_{2n} are formed between existing nodes (they are split pairs moved to the last two 1-factors of $\mathcal{F}_{2n+2}$). These pairs must be rescheduled because they were moved to a different 1-factor (one that did not exist in $\mathcal{F}_{2n}$). If pair (v_{2n+1}, v_{2n+2}) is part of either F_{2n-1} or F_{2n}, one additional node pair between existing nodes must be rescheduled in either F_{2n-1} or F_{2n}, and at least one additional pair must be split in the first $(2n-1)$ 1-factors, thus increasing the total number of schedule changes. Hence, (v_{2n+1}, v_{2n+2}) must be part of the first $(2n-1)$ 1-factors of $\mathcal{F}_{2n+2}$. Each of the existing node pairs that is rescheduled in either F_{2n-1} or F_{2n} requires two schedule changes (one for each existing node), making the total number of schedule changes due to rescheduling of existing node pairs equal to $(4n-4)$.

It is straightforward to observe that $(2n-2)$ split pairs require $(4n-4)$ schedule changes, and four deferred pairs require four scheduled changes (one for each of the existing nodes that is part of a deferred pair). In addition, when there are four deferred pairs, $(2n-2)$ pairs between existing nodes are rescheduled in the last two 1-factors of $\mathcal{F}_{2n+2}$, accounting for $(4n-4)$ schedule changes. Summing over all cases yields the minimum of $(8n-4)$. □

APPENDIX 3

*P*roposition 3: Let $P_R = \{v_1, \ldots, v_{2n-1}\}$ denote an R-path of length $(2n-2)$ on K_{2n}. Let also $v_n \in K_{2n}$ denote the only node that is not part of P_R, and v_{2n+1}, v_{2n+2} denote the newly added nodes when extending the schedule from $\mathcal{F}_{2n}$ to $\mathcal{F}_{2n+2}$. The deferred pairs are formed by (v_n, v_{2n+1}), (v_n, v_{2n+2}), (v_1, v_{2n+1}), and (v_{2n-1}, v_{2n+2}).

Proof: According to Proposition 2, when extending $\mathcal{F}_{2n}$ to F_{2n+2} there exist $(2n-2)$ split pairs. In our algorithm, there pairs are determined by an R-path P_R of length $(2n-2)$ edges (recall that the nodes incident to every link in the R-path represent the split pair. Because the R-path contains each color exactly once, each split pair corresponds to one 1-factor of $\mathcal{F}_{2n}$.). By construction, P_R spans $(2n-1)$ nodes of K_{2n}. Let v_n denote the node of K_{2n} that is not present in P_R. This node is not part of any split pair. Hence, v_n maintains the rendezvous schedule of $\mathcal{F}_{2n}$ for the first $(2n-1)$ 1-factors of $\mathcal{F}_{2n+2}$. Because $\mathcal{F}_{2n+2}$ must be a valid 1-factorization, v_n will rendezvous with newly added nodes v_{2n+1} and v_{2n+2} in the last two 1-factors of $\mathcal{F}_{2n+2}$. Pairs (v_n, v_{2n+1}) and (v_n, v_{2n+2}) are by definition deferred pairs because they consist of one newly added and one existing node and rendezvous on the last two 1-factors of $\mathcal{F}_{2n+2}$.

For the remaining two deferred pairs, we show that newly added nodes v_{2n+1} and v_{2n+2} rendezvous with the endpoints of P_R, i.e., v_1 and v_{2n-1}. This can be easily shown by observing that all nodes in P_R have a degree of two, except for v_1 and v_{2n-1}. The node degree represents the number of split pairs that contain any existing node. An existing node cannot have a degree higher than two, since in this case, more than two split pairs would involve the same node. Recall that all split pairs are scheduled to rendezvous during the last two 1-factors of $\mathcal{F}_{2n+2}$. In order for $\mathcal{F}_{2n+2}$ to be a proper 1-factorization, a node appears on each 1-factor exactly once. Consequently, nodes v_{2n+1} and v_{2n+2} rendezvous with the only nodes of P_R with degree one, that is v_1 and v_{2n-1}. The possible deferred pairs involving v_1 and v_{2n-1} are either (v_1, v_{2n+1}) and (v_{2n-1}, v_{2n+2}) or (v_{2n-1}, v_{2n+1}) and (v_1, v_{2n+2}). □

APPENDIX 4

*P*roposition 4: The broadcast delay of TDBS-SU is $D = \lceil \frac{n}{K} \rceil (2n-1)$ slots.

Proof: To complete a broadcast in the SU mode, the sender must unicast the broadcast message to the remaining $(2n-1)$ broadcast group members. Each of the $(2n-1)$ unicast transmissions takes place in one of the $(2n-1)$ 1-factors of $\mathcal{F}_{2n}$. Each factor requires $\lceil \frac{n}{K} \rceil$ time slots to be completed (here, all transmissions of a 1-factor are completed before transmissions of other 1-factors can proceed, in order to avoid schedule conflicts). Hence, the broadcast delay is equal to $\lceil \frac{n}{K} \rceil$ times the number of 1-factors of $\mathcal{F}_{2n}$. □

APPENDIX 5

*P*roposition 5: The TDBS-AB mode minimizes the broadcast delay when broadcast is realized as a series of concurrent unicast transmissions. This minimum delay is equal to $D = \lceil \frac{n}{K} \rceil \lceil \log_2(2n) \rceil$ slots.

Proof: We first prove that the minimum broadcast delay when broadcast is realized as a series of concurrent unicast transmissions is equal to $D = \lceil \frac{n}{K} \rceil \lceil \log_2(2n) \rceil$ slots. Consider a broadcast group of size $2n$. Assume first that $K \geq n$ (K denotes the number of available channels). Let α_i denote the size of the relay set by the end of slot i, with $\alpha_0 \triangleq 2$ (i.e., the origin node transmits m at slot 0). Because unicast transmissions are used to relay m, a node can relay m to at most one other node. Hence, the relay set can at most double with every slot. Based on this constraint, the maximum number of nodes that could have received m by slot i is equal to $\alpha_i = 2^{i+1}$. The broadcast operation is terminated when all $2n$ nodes are in possession of m. Equating α_i to $2n$ and solving for i yields the slot number at which the broadcast is completed. This is slot $i = \lceil \log_2 n \rceil - 1$. Because our slot numbering starts from zero, the number of slots needed to complete the broadcast is $\lceil \log_2 n \rceil$.

When $K < n$, $\lceil \frac{n}{K} \rceil$ slots are needed to complete one 1-factor. Hence, the mimimim broadcast delay until $2n$ nodes receive the broadcast message is $\lceil \frac{n}{K} \rceil \lceil \log_2(2n) \rceil$. Combining the cases of $K \geq n$ and $K < n$ yields the minimum broadcast delay stated in Proposition 5 (when $K \geq n$, $\lceil \frac{n}{K} \rceil = 1$).

We now show that the AB mode achieves the minimum broadcast delay. Without loss of generality, assume that a broadcast of a message m is initiated by node $F_i(k, 1)$, where $F_i(k, j)$ denotes the node located in the k^{th} row, j^{th} column of 1-factor F_i. With the completion of F_i, the relay set is $R_i^{F_i(k,1)} = \{F_i(k, 1), F_i(k, 2)\}$. In the splitting algorithm, nodes $F_i(k, 1)$ and $F_i(k, 2)$ appear in adjacent rows (due to the cyclic nature of Algorithm 3, rows 1 and 8 are considered adjacent) on 1-factor F_{i+1}. Because the pair $(F_i(k,1), F_i(k,2))$ appears on separate rows of F_{i+1}, each node will relay m to two new nodes.

Further execution of the splitting algorithm divides the nodes in the relay set $R_{i+1}^{F_i(k,1)}$ to four adjacent rows. Since none of the nodes in $R_{i+1}^{F_i(k,1)}$ appears on the same row, the relay set after the completion of factor F_{i+1} increases to eight nodes. Following the recursive application of the splitting algorithm, the relay set after the completion of $\lfloor \log_2(2n) \rfloor$ 1-factors has a size of $2^{\lfloor \log_2 2n \rfloor}$. If $\lfloor \log_2(2n) \rfloor = \log_2(2n)$, the broadcast is complete since $2^{\log_2(2n)} = 2n$. Otherwise, one extra 1-factor is needed to relay the broadcast to the remaining $2n - 2^{\lfloor \log_2(2n) \rfloor}$ nodes. Because $2^{\lfloor \log_2(2n) \rfloor} > n$, the splitting algorithm places n nodes from the relay set into the n rows of the $\lfloor \log_2 2n \rfloor + 1 = \lceil \log_2(2n) \rceil$th 1-factor. These n relays complete the broadcast operation. Combining the two cases yields the required number of 1-factors to be equal to $\lceil \log_2(2n) \rceil$. Proposition 5 follows by noting that every 1-factor requires $\lceil \frac{n}{k} \rceil$ slots to be completed. □

Appendix 6

*P*roposition 6: In the presence of an external jammer, the expected number $\mathrm{E}[Z]$ of 1-factorizations needed to complete a broadcast operation in the SU mode is,

$$\begin{aligned}\mathrm{E}[Z] &= (1-p)^{2n-1} + \sum_{i=2}^{\infty} i(1-p^{i-1})^{2n-1} \times \\ &\quad \sum_{k=1}^{2n-1} \binom{2n-1}{k} \left(\frac{p^{i-1}(1-p)}{1-p^{i-1}}\right)^k, \end{aligned} \quad (2)$$

where $p = \frac{J}{K}$ denotes the jamming probability.

Proof: Suppose that an arbitrary node v_j attempts a broadcast transmission in the presence of an external jammer. This broadcast is completed in a single 1-factorization if the jammer is unsuccessful in jamming the communication of v_j for $(2n-1)$ consecutive slots. Because h_j is uniformly distributed, v_j's transmission on a given slot is successful with probability $\left(1 - \frac{J}{K}\right)$. Moreover, the success/failure events are independent from one slot to another and for every node. Hence,

$$\Pr[Z=1] = \left(1 - \frac{J}{K}\right)^{2n-1} = (1-p)^{2n-1}.$$

The broadcast is completed in two 1-factorizations if every receiver is jammed at most one time, and at least one receiver is jammed on the first 1-factorization. Taking into account all possible combinations,

$$\Pr[Z=2] = \sum_{k=1}^{2n-1} \binom{2n-1}{k} (1-p)^{2n-1-k} p^k (1-p)^k.$$

Generalizing to the case of $Z = i$, it follows that,

$$\begin{aligned}\Pr[Z=i] &= \sum_{k=1}^{2n-1} \binom{2n-1}{k} (1-p^{i-1})^{2n-1-k} \\ &\quad p^{(i-1)k}(1-p)^k, \\ &= (1-p^{i-1})^{2n-1} \sum_{k=1}^{2n-1} \binom{2n-1}{k} \\ &\quad \left(\frac{p^{i-1}(1-p)}{1-p^{i-1}}\right)^k.\end{aligned}$$

Proposition 6 follows from the definition of the expectation, i.e., $\mathrm{E}[Z] = \sum_i i \Pr[Z=i]$. □

Appendix 7

*P*roposition 7: Let the per-slot jamming probability be equal to $p = \frac{1}{K}$, and let $K \geq n$. After the first successful relay of a broadcast message m, the broadcast delay D_2 until m is received by $(2n-2)$ nodes (all nodes, but one) is bounded by,

$$\lceil \log_2(2n) \rceil - 1 \leq D_2 \leq \lceil \log_2(2n) \rceil. \quad (3)$$

Proof: The lower bound immediately follows from Proposition 5. The broadcast delay in the absence of a jammer is equivalent to the delay in the presence of an external jammer who is unsuccessful in jamming any communicating pair for $\lceil \log_2(2n) \rceil - 1$ slots. Hence, after the first successful relay, the lower bound on D_2 follows.

To compute the upper bound on D_2, assume that an arbitrary node j wants to broadcast a message m to the remaining $(2n-1)$ nodes. Note that because $K \geq n$ every 1-factor is completed at one time slot. Let a_i denote the size of the relay set at slot i. Initially, $a_0 = 2$, i.e., node j has completed its first successful relay. Once $a_i \geq 2$, the adversary can jam at most one of the pairs relaying m. The size of the relay set in this worst-case scenario grows according to the formula.

$$a_i = 2a_{i-1} - 1 = 2^i + 1, \; i \leq \lceil \log_2(2n) \rceil - 1, \quad (4)$$

where a_i is computed recursively with $a_0 = 2$. To show the validity of (4), we refer to the proof of Proposition 5, where we showed that for $a_i \leq n$, the size of the relay set doubles with the increment of i. Because the adversary jams at most one frequency band per time slot, in the worst case, $a_i = 2a_{i-1} - 1$. This is true until $a_i \geq n$, in which case the size of the relay set can no longer double. In slot i, $i \leq \lceil \log_2(2n) \rceil - 1$, the relay set becomes larger than n for the first time. That is, it takes $i = \lceil \log_2(2n) \rceil - 1$ slots until more than half the nodes can relay message m. These $a_i \geq n$ relay nodes communicate with the remaining $2n - 2^i - 1 \leq n$ nodes that have not yet received m. Since only one frequency band is jammed, the number of nodes that have received m at the end of slot $(i+1)$ is equal to $(2n-2)$. In this worst case, only one node has not received m after $\lceil \log_2(2n) \rceil$ slots. □

APPENDIX 8

Proposition 8: Under the compromise of r nodes, the jamming probability p is bounded by,

$$\min\{1, \frac{J}{K - \lceil \frac{r}{2} \rceil}\} \leq p \leq \min\{1, \frac{J}{K-r}\}. \tag{5}$$

Proof: Let x be the number of frequency bands over which the r compromised nodes are scheduled to communicate according to 1-factor F. The number of bands over which legitimate communications take place in each slot is reduced to $(K-x)$. This is due to the fact that the frequency bands assigned to every 1-factor are permutation of the set of bands $\mathcal{C}$. Hence, the jamming probability is increased to $p = \frac{J}{K-x}$. To derive bounds on p, we consider the lowest and highest values of x. If the compromised nodes are scheduled to communicate with each other at 1-factor F, then $x = x_{\min} = \lceil \frac{r}{2} \rceil$, where the ceiling function is used to account for an odd r. This value of x yields the lower bound on p. On the other hand, if all r nodes are scheduled to communicate with legitimate ones (appear on separate rows in F), then $x = x_{\max} = r$, and p attains its maximum value. Note that $p \leq 1$ and hence, $r \leq K - J$. When r is larger than $K-J$, there are 1-factors where all transmissions are jammed with certainty. □

APPENDIX 9

Proposition 10: Under the compromise of r border nodes of a cluster i, $\mathrm{E}[D_e]$ is given by,

$$\mathrm{E}[D_e] = \frac{1}{1 - \left(P_c^{N_L} + \sum_{i=1}^{N_L} \binom{N_L}{i} \left(\frac{J(1-P_c)}{K-r} \right)^i \right)^{N_C}}, \tag{6}$$

where $P_c = \frac{r}{N_C \times N_L}$ denotes the compromise probability.

Proof: At each time slot, the probability that an adjacent cluster fails to receive a broadcast is due to: (a) all N_L links are shared with compromised border nodes, and (b) the links shared with uncompromised border nodes are jammed by the adversary. So the probability that a neighboring cluster fails to receive a broadcast is,

$$P_{fail} = (P_c)^{N_L} + \sum_{i=1}^{N_L} \binom{N_L}{i} \left(\frac{J(1-P_c)}{K-r} \right)^i.$$

The probability that at least one of the neighboring clusters successfully receive the broadcast at a time slot is,

$$P_{success} = 1 - (P_{fail})^{N_C}.$$

The broadcast among adjacent nodes forms a Bernoulli trial with a success probability $P_{success}$, so the average delay until the first success is $1/P_{success}$, which leads to our result. □

APPENDIX 10

Proposition 11: Under the compromise of r nodes, $\mathrm{E}[DIV]$ is given by,

$$\mathrm{E}[DIV] = 1 - (P_c)^{N_L}. \tag{7}$$

Proof: For any neighboring cluster, the probability that it can not receive a broadcast is equivalent to the probability of all N_L links contain at least one compromised border node. This probability is $(P_c)^{N_L}$. So the expected number of neighboring clusters that can get a broadcast is $N_C \cdot (1 - (P_c)^{N_L})$. Dividing this value with N_C, yields $\mathrm{E}[DIV]$. □