Fast and Secure Rendezvous Protocols for Mitigating Control Channel DoS Attacks

Mohammad J. Abdel-Rahman, Hanif Rahbari, and Marwan Krunz
Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, USA

Philippe Nain
INRIA, Sophia Antipolis, France

***Abstract*—The operation of a wireless network relies extensively on exchanging messages over a universally known channel, referred to as the *control channel*. The network performance can be severely degraded if a jammer launches a denial-of-service (DoS) attack on such a channel. In this paper, we design quorum-based frequency hopping (FH) algorithms that mitigate DoS attacks on the control channel of an asynchronous ad hoc network. Our algorithms can establish unicast as well as multicast communications under DoS attacks. They are fully distributed, do not incur any additional message exchange overhead, and can work in the absence of node synchronization. Furthermore, the multicast algorithms maintain the multicast group consistency. The efficiency of our algorithms is shown by analysis and simulations.**

I. Introduction

Wireless communications are vulnerable to intentional interference attacks, typically referred to as jamming. The performance of a wireless network can be severely degraded if a jammer launches a denial-of-service (DoS) attack on the control channel. Conventional anti-jamming techniques often rely on spread spectrum communications, including frequency hopping (FH). FH has been used in the literature for establishing unicast communications in dynamic spectrum access (DSA) networks, where a common control channel does not always exist. However, most existing FH designs are based on ad hoc approaches that do not provide any performance guarantees. One way to construct FH sequences in a systematic manner is to use quorum systems [3]. Quorum-based FH designs are advantageous in ad hoc networks because of their robustness to synchronization errors [4]. However, previous quorum-based FH designs, such as [3], do not support *multicast rendezvous*, where all the nodes in a multicast group are required to meet in the same time slot.

The authors in [6] proposed an FH-based jamming-resistant broadcast communication scheme. In their scheme, the broadcast operation is implemented as a series of unicast transmissions, which can lead to multicast inconsistency. For example, a group of nodes may share a *group key* that is used to encode/decode common secure communication messages. For security purposes, this key may have to be updated periodically [7]. However, the change in the group key has to be consistent among all nodes in the group. Even with the jamming resiliency, such consistency cannot be guaranteed if changes in the group key are conveyed sequentially. Instead of designing different FH sequences that overlap at common slots, the multicast rendezvous in [5] is established after a series of pairwise rendezvous operations that result in tuning all nodes in the multicast group to a common FH sequence. The effectiveness of this approach cannot be maintained under node compromise (if one node is compromised, then the FH sequences of all nodes are exposed). The authors in [1] were the first to consider multicast rendezvous in fast-varying DSA networks, using different FH sequences while maintaining multicast consistency.

In this paper, we present three FH algorithms to maintain control communications under a DoS attack on the control channel. More specifically, we propose a novel nested grid quorum-based FH algorithm, called NUDoS, for establishing unicast communications in a hostile environment with multiple jammers. NUDoS is faster than previously proposed pairwise rendezvous algorithms, robust to node compromise, and can function in the absence of synchronization. Next, to establish multicast communications while guaranteeing multicast consistency, we customize the two multicast rendezvous algorithms (AMQFH and nested-CMQFH) proposed in [1]. We call the modified algorithms KMDoS and NCMDoS, respectively. KMDoS and NCMDoS provide different tradeoffs between speed and robustness to node compromise. Our algorithms are distributed and do not incur any additional message overhead.

The rest of this paper is organized as follows. Section II introduces our models, defines our metrics, and states our problem. The NUDoS algorithm is presented in Section III. Section IV briefly introduces the KMDoS and NCMDoS algorithms. We evaluate our algorithms in Section V, and conclude the paper in Section VI.

II. Models, Metrics, and Problem Statement

A. System Model

We consider a wireless ad hoc network with k nodes and L channels, denoted by $f_1, f_2, \ldots, f_L$. Without loss of generality, we assume that FH occurs on a per-slot basis, where the slot duration is T seconds. A packet can be exchanged between two or more nodes if they hop onto the same channel in the same time slot. We assume that one time slot is sufficient to exchange one message. If multiple groups happen

This research was supported in part by NSF (under grants CNS-1016943 and CNS-0904681, IIP-0832238, IIP-1231043), Raytheon, and the "Connection One" center. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

978-1-4673-5946-7/13/$31.00 ©2013 IEEE

to meet on the same channel in the same time slot, they use a CSMA/CA-style procedure to resolve contention.

For $j = 1, \ldots, k$, each node j has its unique FH sequence $\boldsymbol{w}^{(j)}$. The channel used in the ith slot of FH sequence $\boldsymbol{w}^{(j)}$ is denoted by $w_i^{(j)}, w_i^{(j)} \in \{f_1, \ldots, f_L\}$. Channel f_j is called a *rendezvous frequency* for the FH sequences $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(k)}$ if there exists a *rendezvous slot* i such that $w_i^{(m)} = f_j, \forall m \in \{1, \ldots, k\}$. In our setup, each FH sequence consists of several frames. Each frame consists of a block of time-frequency hops.

B. Attack Model

We consider two types of attacks: an insider attack in which an attacker can compromise a legitimate node and extracts its FH sequence, and a Markovian jamming attack where a jammer follows a two-state discrete-time Markov process. When the jammer is in state 0 it does not transmit; otherwise, it transmits a jamming signal. Let $\rho^{(m)}$ be the probability that channel m is in state 1, and let $\mathcal{T}_1^{(m)}$ be the expected time (in slots) that channel m spends in state 1 before returning to state 0. Then, the transition probabilities from state 0 to state 1 ($p^{(m)}$) and from state 1 to state 0 ($q^{(m)}$) can be expressed as:

$$p^{(m)} = \frac{\rho^{(m)}}{1-\rho^{(m)}} \frac{1}{\mathcal{T}_1^{(m)}}, \quad q^{(m)} = \frac{1}{\mathcal{T}_1^{(m)}}. \tag{1}$$

C. Evaluation Metrics

Our algorithms are evaluated according to two metrics: expected evasion delay (ED) and expected Hamming distance (HD). ED is defined as the time between the successful jamming of the control channel and the re-establishment of a new one. The expected ED is considered because of the existence of a randomly assigned part in our FH sequences. The expected HD for two FH sequences $\boldsymbol{x} = (x_1 \ldots x_n)$ and $\boldsymbol{y} = (y_1 \ldots y_n)$ is defined as $E[\left(\sum_{i=1}^{n} \mathbf{1}_{\{x_i \neq y_i\}}\right)/n]$, where $\mathbf{1}_{\{\cdot\}}$ is the indicator function and n is the frame length. In addition to robustness to node compromise, FH sequences with higher HD will have a lower collision probability. A collision occurs when two or more neighboring groups meet on the same channel in the same time slot.

D. Problem Statement

The FH construction problem is stated as follows: *Given $f_1, \ldots, f_L$, k, and n, determine the values of $w_i^{(j)}, 1 \leq i \leq n, 1 \leq j \leq k$, that result in the minimum ED, and achieve a minimum HD of d.* This problem is formulated as follows:

$$\underset{\{w_i^{(j)}: 1 \leq i \leq n, 1 \leq j \leq k\}}{\text{minimize}} \quad l$$

$$\text{Subject to.} \quad w_l^{(i)} = w_l^{(j)}, \forall i, j \in \{1, \ldots, k\}, i \neq j \tag{2}$$

$$s_i^{(l)}[w_l^{(i)}] = 0, \forall i \in \{1, \ldots, k\} \tag{3}$$

$$\sum_{r=1}^{n} \mathbf{1}_{\{w_r^{(i)} \neq w_r^{(j)}\}} \geq nd, \forall i, j \in \{1, \ldots, k\}, i \neq j \tag{4}$$

where $s_i^{(r)}[f_x] \in \{0, 1\}$ is the state of frequency $f_x \in \{f_1, \ldots, f_L\}$ in the rth time slot, as seen by node i. Assume that $s_i^{(r)}[f_x], i \in \{1, \ldots, k\}, r \in \{1, \ldots, n\}, x \in \{1, \ldots, L\}$ are given. Then, the solution to Problem 1 gives the minimum ED, denoted by ED^*, and the rendezvous frequency, denoted by f_{u^*}. ED^* and u^* are given by:

$$ED^* = \min_{1 \leq u \leq L} \left\{ \min_{1 \leq r \leq n} \left(\bigvee_{i=1}^{k} s_i^{(r)}[f_u] == 0 \right) \right\} \tag{5}$$

$$u^* = \underset{1 \leq u \leq L}{\operatorname{argmin}} \left\{ \min_{1 \leq r \leq n} \left(\bigvee_{i=1}^{k} s_i^{(r)}[f_u] == 0 \right) \right\} \tag{6}$$

where $\bigvee$ denotes the logical OR operation.

Relaxing the assumption of knowing the future states of the channels, next we propose a centralized algorithm that solves the above problem in $\mathcal{O}(knL)$ time, assuming that only the channel's transition probabilities are known.

The centralized algorithm, which relies on predicting the future states of the channels given the current states, can be summarized by the following steps:

1) For each slot $j = 1, \ldots, n$, compute p_j^* and l_j^* as follow:

$$p_j^* = \max_{1 \leq l \leq L} \left\{ \prod_{i=1}^{k} p_{n-e+j}^{(l)}(s_i^{(e)}[f_l], 0) \right\} \tag{7}$$

$$l_j^* = \underset{1 \leq l \leq L}{\operatorname{argmax}} \left\{ \prod_{i=1}^{k} p_{n-e+j}^{(l)}(s_i^{(e)}[f_l], 0) \right\} \tag{8}$$

where e is the index of the slot in the current frame when channel f_l has been recently sensed and $p_{n-e+j}^{(l)}(s_i^{(e)}[f_l], 0)$ is the $(n-e+j)$-step transition probability of f_l form state $s_i^{(e)}[f_l]$ to state 0. In general, the v-step transition probability of channel m from state s to state 0 can be expressed as:

$$p_v^{(m)}(s, 0) = \frac{q^{(m)} + p^{(m)}\left[-\frac{q^{(m)}}{p^{(m)}}\right]^s \left[1 - p^{(m)} - q^{(m)}\right]^v}{p^{(m)} + q^{(m)}}. \tag{9}$$

2) Sort slots ascendingly according to their p_j^* values.
3) Select the top $n - \lceil nd \rceil = \lfloor n(1-d) \rfloor$ slots in the list, and assign frequency $f_{l_j^*}$ to slot j in all FH sequences.
4) For the remaining $\lceil nd \rceil$ slots, assign different frequencies for different FH sequences.

Next, we exploit some properties of quorum systems in designing distributed FH rendezvous algorithms.

III. Unicast Communications

Before describing NUDoS for unicast communications, we first give a few basic definitions.

A. Preliminaries

Definition 1. *Given a set $Z_n = \{0, 1, \ldots, n-1\}$, 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. *Given a non-negative integer i and a quorum G in a quorum system Q under Z_n, we define $rotate(G, i) =$*

$\{(x+i) \mod n, x \in G\}$ *to denote a cyclic rotation of quorum* G *by* i.

Definition 3. *A quorum system* Q *under* Z_n *is said to satisfy the rotation* k*-closure property for some* $k \geq 2$ *if* $\forall G_1, \ldots, G_k \in Q$ *and* $\forall i_1, \ldots, i_k \in Z_n$, $\bigcap_{j=1}^{k} rotate(G_j, i_j) \neq \emptyset$.

Quorum systems that enjoy the above rotation k-closure property can be exploited to achieve asynchronous communications. One such quorum system that satisfies the rotation 2-closure property is the grid quorum system [4].

Definition 4. *A grid quorum system* [4] *arranges the elements of the set* Z_n *as a* $\sqrt{n} \times \sqrt{n}$ *array. In this case, a quorum is formed from the elements of any column plus any row of the grid.*

Figure 1 illustrates the rotation closure property for two quorums G and H in a grid quorum system Q under Z_{16}. One quorum's column must intersect with the other quorum's row, and vice versa. Hence, the two quorums have at least two intersections (labeled I in Figure 1). In Figure 1, $G' = rotate(G, 1)$ and $H' = rotate(H, 2)$ intersect at the two elements labeled as I'. Hence, the grid quorum system satisfies the rotation 2-closure property.

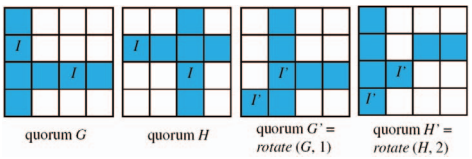


Fig. 1: Rotation 2-closure property of grid quorum systems.

B. NUDoS Algorithm

In NUDoS, every frame of every FH sequence uses $\sqrt{n}-1$ rendezvous frequencies, where n is the frame length in slots. The following example explains the operation of the NUDoS algorithm for $n = 16$ (hence, each frame of every FH sequence contains $\sqrt{n}-1 = 3$ rendezvous frequencies).

1) Construct a grid quorum system Q under Z_{16}. Q consists of 16 different quorums, each of $2\sqrt{16}-1 = 7$ elements.
2) Construct an FH sequence $\boldsymbol{w}$ as follows:
   - Select *the outer-most quorum* $G_1^{(1)}$ from the quorum system Q (e.g., $G_1^{(1)} = \{0, 1, 2, 3, 4, 8, 12\}$, where each entry represents the index of a time slot in a 16-slot frame).
   - Assign a rendezvous frequency $h_1^{(1)} \in \{f_1, \ldots, f_L\}$ to the FH slots that correspond to $G_1^{(1)}$.
   - Delete quorum $G_1^{(1)}$ from the original 4×4 grid and select the *next outer-most quorum* $G_2^{(1)}$ from the resulting 3×3 grid (e.g., $G_2^{(1)} = \{6, 9, 10, 11, 14\}$). Then, assign another rendezvous frequency $h_2^{(1)}$ to the FH slots that correspond to $G_2^{(1)}$.
   - Delete quorum $G_2^{(1)}$ from the 3×3 grid, and select the next outer-most quorum $G_3^{(1)}$ from the resulting 2×2 grid (e.g., $G_3^{(1)} = \{7, 13, 15\}$). Then, assign a third rendezvous frequency $h_3^{(1)}$ to the FH slots that correspond to $G_3^{(1)}$.
   - Assign a random frequency $h_x^{(1)} \in \{f_1, \ldots, f_L\} \setminus \{h_1^{(1)}, h_2^{(1)}, h_3^{(1)}\}$ to each of the unassigned slots.
   - Repeat the above steps for the other frames in $\boldsymbol{w}$.
3) Repeat step 2 for other FH sequences.

Throughout this paper, $h_i^{(j)}$ and $G_i^{(j)}$, $i \in \{1, \ldots, \sqrt{n}-1\}$, denote the ith quorum-assigned frequency that is assigned to the $(\sqrt{n}-i+1) \times (\sqrt{n}-i+1)$ quorum $G_i^{(j)}$ in the jth frame.

C. Features of the NUDoS Algorithm

NUDoS has two main features. First, because of the nested generation of quorums, the *overlap ratio* between two FH sequences (number of rendezvous slots in a frame divided by the frame length) is significantly higher than the overlap ratio for a non-nested grid quorum-based FH algorithm (herein denoted by UDoS). In UDoS, an FH sequence consists of only one rendezvous frequency, assigned to a $\sqrt{n} \times \sqrt{n}$ quorum. FH systems with a higher overlap ratio work more efficiently in hostile environments, where a jammer may suddenly appear on a rendezvous channel. Besides having a higher overlap ratio, NUDoS involves multiple rendezvous frequencies per frame, which increases the likelihood of rendezvousing.

The advantage of a nested grid quorum with multiple rendezvous frequencies can be formalized by deriving the expected overlap ratio for UDoS and NUDoS, denoted by $\mathcal{V}_{UDoS}$ and $\mathcal{V}_{NUDoS}$, respectively. $\mathcal{V}_{UDoS}$ is composed of the sum of two parts; the expected overlap ratio between the quorum-based assigned parts of the FH sequences, denoted by $\mathcal{V}_{UDoS}^{Q}$, and the expected overlap ratio between the randomly assigned parts, denoted by $\mathcal{V}_{UDoS}^{R}$. Similarly, $\mathcal{V}_{NUDoS}$ is composed of $\mathcal{V}_{NUDoS}^{Q}$ and $\mathcal{V}_{NUDoS}^{R}$. For a given n, $\mathcal{V}_{UDoS}^{Q}$ and $\mathcal{V}_{NUDoS}^{Q}$ can be determined numerically. After some manipulations, $\mathcal{V}_{UDoS}^{R}$ and $\mathcal{V}_{NUDoS}^{R}$ can be expressed as follows:

$$\mathcal{V}_{UDoS}^{R}(L, n) = \frac{(\sqrt{n}-1)^2}{L}\left\{2 - \frac{(\sqrt{n}-1)^2}{n}\right\} \quad (10)$$

$$\mathcal{V}_{NUDoS}^{R}(L, n) = \frac{1}{L}\left\{2 - \frac{1}{n^2}\right\}. \quad (11)$$

Plotting $\mathcal{V}_{UDoS}$ and $\mathcal{V}_{NUDoS}$ vs. n, one can see that $\mathcal{V}_{NUDoS}$ is larger than $\mathcal{V}_{UDoS}$, and both decrease with n.

The second attractive feature of NUDoS is its robustness to node compromise. Because the quorum-based assigned part of the FH sequence is the part that is intended to support the rendezvous capability, if this part is compromised, the rendezvous capability may be eliminated or reduced significantly. NUDoS sequences are composed of $\sqrt{n}-1$ nested quorums that are generally different for different frames in a given FH sequence, and also different for different FH sequences. Hence, if a node is compromised and its FH sequence is exposed, less information will be leaked about other FH sequences, compared with UDoS sequences. The number of different channel assignments for a given n ($\mathcal{K}_n$) is given by:

$$\mathcal{K}_n = \prod_{j=0}^{\sqrt{n}-2} (\sqrt{n}-j)^2. \quad (12)$$

IV. Multicast Communications

The multicast rendezvous algorithms, AMQFH and CMQFH, proposed in [1] are customized for maintaining multicast communications under a DoS attack on the control channel. The resulted algorithms are called KMDoS and CMDoS, respectively. These algorithms have two main attractive features. First, they allow a node to construct its sequence by only knowing the number of nodes in its multicast group. Hence, they can be executed in a fully distributed way. Second, these algorithms can still function in the absence of node synchronization. Due to space limitations, the details of these algorithms are not mentioned here, but can be found in [2].

We evaluate KMDoS and CMDoS based on the expected ED and HD. KMDoS and CMDoS are implemented in a distributed way as follows. First, the source node uses a series of pairwise rendezvous to communicate the number of nodes in the multicast group to the target multicast group. Then, each receiving node constructs its own multicast FH sequence.

A. Expected ED

The expected ED of KMDoS and CMDoS, denoted by $\mathcal{E}_k$ and $\mathcal{E}_c$, respectively, can be expressed as follows:

Result 1. *$\mathcal{E}_k$ is given by:*

$$\mathcal{E}_k = \sum_{i=1}^{n-1}\left[i\Gamma(\gamma_{i+1})\prod_{j=1}^{i}(1-\Gamma(\gamma_j))\right] \tag{13}$$

where $\Gamma(\gamma_i)$ is the probability that slot i is a rendezvous slot and γ_i is the probability that slot i is a quorum slot (i.e., assigned a rendezvous frequency). $\Gamma(\gamma_i)$ and $\gamma_i, i = 1, \ldots, n-1$, are given by ($k$ is the multicast group size minus one for KMDoS):

$$\Gamma(\gamma_j) = \sum_{i=0}^{k}\left[\binom{k+1}{i}\gamma_j^{k+1-i}\left(\frac{1-\gamma_j}{L}\right)^i\right] + \left(\frac{1}{L}\right)^k(1-\gamma_j)^{k+1} \tag{14}$$

$$\gamma_i = \frac{\left\lfloor\frac{kn}{k+1}\right\rfloor - i + 2}{n} + \frac{i-1}{n}\times\frac{\left\lfloor\frac{kn}{k+1}\right\rfloor - i + 3}{n-i+1}. \tag{15}$$

Result 2. *$\mathcal{E}_c$ is given by:*

$$\mathcal{E}_c = \Theta\sum_{i=1}^{n-1} i(1-\Theta)^i \tag{16}$$

where Θ is the probability that a given slot is a rendezvous slot. Θ is given by (k is the multicast group size for CMDoS):

$$\Theta = \sum_{i=0}^{k-1}\left[\left(\frac{1}{L}\right)^i\sum_{\substack{\forall\{e_1,\ldots,e_{k-i}\}\\ \in\{p_1,\ldots,p_k\}}}\frac{\prod_{j=k-i+1}^{k}(e_j-1)/e_j}{e_1\ldots e_{k-i}}\right] + \left(\frac{1}{L}\right)^{k-1}\prod_{l=0}^{k-1}\frac{e_l-1}{e_l}. \tag{17}$$

Plotting $\mathcal{E}_k$ and $\mathcal{E}_c$, one can see that for $L > 3$, $\mathcal{E}_c \gg \mathcal{E}_k$. Both, $\mathcal{E}_c$ and $\mathcal{E}_k$ increases with the multicast group size.

B. Expected HD

Result 3. *Let $\phi \stackrel{def}{=} n - \left\{\left\lfloor\frac{kn}{k+1}\right\rfloor + 1\right\}$. Then, the expected HD of KMDoS, denoted by $\mathcal{H}_k$, and its upper bound value, denoted by $\mathcal{H}_{k,best}$, are given by:*

$$\mathcal{H}_k = \frac{L-1}{nL}\left\{\frac{(\varphi-1)(\phi+1)}{\varphi} + \frac{\phi}{\varphi}\right\} \tag{18}$$

$$\mathcal{H}_{k,\text{best}} = \frac{\phi+1}{n} \tag{19}$$

where $\mathcal{H}_{k,best}$ corresponds to the case when different nodes select different sequences, and nodes cannot rendezvous during the randomly assigned slots. $\mathcal{H}_k$ represents the case when nodes can select different sequences or the same sequence.

Result 4. *The expected HD of CMDoS, denoted by $\mathcal{H}_c$, and its upper bound value, denoted by $\mathcal{H}_{c,best}$, are given by:*

$$\mathcal{H}_c = \frac{L-1}{2Lk^2}\sum_{i=1}^{k}\sum_{j=1}^{k}\left(1-\frac{1}{p_ip_j}\right) \tag{20}$$

$$\mathcal{H}_{c,\text{best}} = \frac{1}{2\binom{k}{2}}\sum_{i=1}^{k}\sum_{\substack{j=1\\ j\neq i}}^{k}\left(1-\frac{1}{p_ip_j}\right) \tag{21}$$

where $\mathcal{H}_{c,best}$ is defined similar to $\mathcal{H}_{k,best}$.

Note that as the multicast group size increases, $\mathcal{H}_c$ increases but $\mathcal{H}_k$ decreases, and hence the gap between $\mathcal{H}_c$ and $\mathcal{H}_k$ increases with the increase in the size of the multicast group.

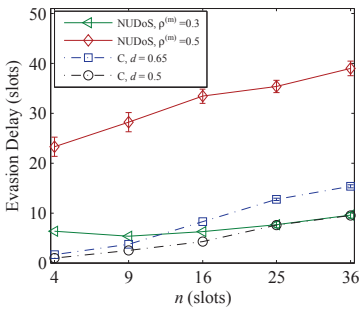
CMDoS is robust against node compromise but it is slow. To reduce the ED of CMDoS, we augment it with a nesting design similar to the NUDoS algorithm, as discussed [2]. The nested version of CMDoS is called NCMDoS.

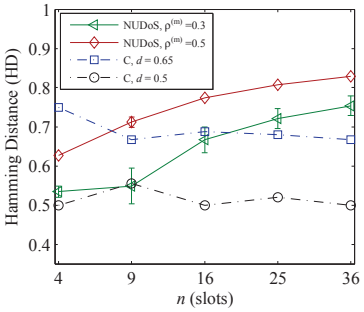
Remark 1. FH sequences constructed according to NUDoS, KMDoS, and NCMDoS can establish asynchronous communications if each FH sequence continues to use the same outer-most quorum and channel in all frames of the FH sequence. This condition is sufficient but not necessary. Thus, FH sequences can still rendezvous even if the outer-most quorum is changed in some frames, provided that this change does not occur very frequently.

Remark 2. In Section V, channels and quorums are selected based on the forecasted availability of the channels at different quorums, as derived from the jamming model described in Section II-B. A channel is considered available at a future slot if it is predicted to be available at that slot with probability greater than p_{th}. The details of the channel and quorum selection procedures are omitted due to space limitation.

V. Performance Evaluation

We now present simulation results for the NUDoS, KMDoS, and NCMDoS algorithms, and compare them with the centralized algorithm. The proposed algorithms are studied under different jamming probabilities ($\rho^{(m)}$), as well as different frame lengths and group sizes for unicast and multicast, respectively. Our evaluation metrics are the ED and the HD. Our algorithms are simulated under a realistic setting of no synchronization (the misalignment between FH sequences is





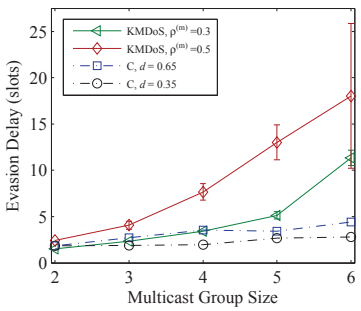


Fig. 2: ED for NUDoS ($p_{th} = 0.5, \mathcal{T}_1^{(m)} = 8$). Fig. 3: HD for NUDoS ($p_{th} = 0.5, \mathcal{T}_1^{(m)} = 8$). Fig. 4: ED for KMDoS ($p_{th} = 0.5, \mathcal{T}_1^{(m)} = 8$).

randomly selected in each experiment). The 95% confidence intervals are indicated. To achieve a minimum HD of d in the centralized algorithm, the actual HD (i.e., $\lfloor nd \rfloor / n$) might be different for different frame lengths.

A. Unicast Communications (NUDoS)

Figure 2 depicts the ED of NUDoS, and compare it with the centralized algorithm (denoted by C). The ED for both algorithms (NUDoS and C) increases with n because of the reduction in the overlap ratio. The ED also increases with $\rho^{(m)}$. While achieving a close HD to the centralized algorithm for small to moderate values of $\rho^{(m)}$, the speed of NUDoS is comparable to the centralized algorithm. Increasing d in (4) increases the ED of the centralized algorithm.

The HD for NUDoS and C is plotted in Figure 3. The HD of NUDoS increases with n because of the reduction in the overlap ratio. It also increases with $\rho^{(m)}$ because of the increase in the number of unassigned slots (in our simulations, each unassigned slot increments the HD by $1/n$).

B. Multicast Communications (KMDoS and NCMDoS)

Figure 4 shows the ED of KMDoS and the centralized algorithm. The ED of KMDoS increases with the group size for large values of $\rho^{(m)}$. Figure 5 depicts the ED of NCMDoS vs. $\rho^{(m)}$ for a group of size 3. NCMDoS is much slower than both KMDoS and the centralized algorithm.

As shown in Figure 6, the HD of NCMDoS is larger than that of KMDoS, and the gap increases with the increase in the group size. The HD increases with $\rho^{(m)}$ because of the increase in the number of unassigned slots.

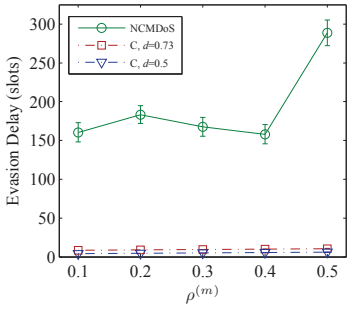


Fig. 5: ED for NCMDoS (group size = 3, $p_{th} = 0.5, \mathcal{T}_1^{(m)} = 8$).

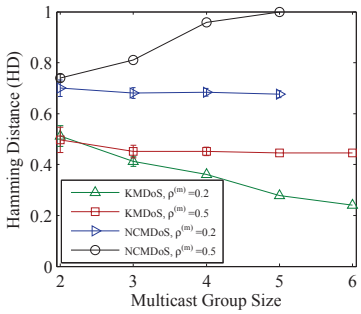


Fig. 6: HD for KMDoS and NCMDoS ($p_{th} = 0.5, \mathcal{T}_1^{(m)} = 4$).

VI. Conclusions

In this paper, we designed three FH algorithms for establishing unicast (NUDoS) and multicast (KMDoS and NCMDoS) communications in the presence of a control channel DoS attack. KMDoS and NCMDoS maintain the multicast consistency, and provide different tradeoffs between speed and robustness to node compromise. Our algorithms are distributed, do not incur additional message exchange overhead, and work in the absence of synchronization. We simulated our algorithms under a realistic setting of no synchronization.

References

[1] M. J. Abdel-Rahman, H. Rahbari, and M. Krunz, "Adaptive frequency hopping algorithms for multicast rendezvous in DSA networks," in *Proc. of the IEEE DySPAN Conf.*, Oct. 2012, pp. 436–447.

[2] M. J. Abdel-Rahman, H. Rahbari, M. Krunz, and P. Nain, "Fast and secure rendezvous protocols for mitigating control channel DoS attacks," University of Arizona, Tech. Rep. TR-UA-ECE-2012-4, Jan. 2013. [Online]. Available: http://www2.engr.arizona.edu/~mjabdelrahman.

[3] K. Bian, J. M. Park, and R. Chen, "A quorum-based framework for establishing control channels in dynamic spectrum access networks," in *Proc. of the ACM MobiCom Conf.*, 2009, pp. 25–36.

[4] J.-R. Jiang, Y.-C. Tseng, C.-S. Hsu, and T.-H. Lai, "Quorum-based asynchronous power-saving protocols for IEEE 802.11 ad-hoc networks," *Mobile Networks and Applications*, vol. 10, pp. 169–181, Feb. 2005.

[5] Z. Lin, H. Liu, X. Chu, and Y.-W. Leung, "Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks," in *Proc. of the IEEE INFOCOM Conf.*, 2011, pp. 2444–2452.

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

[7] D. R. Stinson, *Cryptography: Theory and Practice*. Chapman and Hall/CRC, Taylor and Francis Group, 2006.