Randomized Channel Hopping Scheme for Anti-Jamming Communication

Eun-Kyu Lee, Soon Y. Oh, and Mario Gerla
Computer Science Department
University of California at Los Angeles, Los Angeles, CA, USA
{eklee, soonoh, gerla}@cs.ucla.edu

***Abstract*—Jamming attacks have been recently studied as wireless security threats disrupting reliable RF communication in a wireless network. By emitting noise-like signals arbitrarily on the shared wireless medium, a jammer can easily disturb the network. Countermeasures such as Frequency-Hopping Spread Spectrum enable nodes to avoid the jamming attacks by hopping over multiple channels. However, these solutions require pre-key establishment before data transmission, which in turns introduces several constraints. In order to solve the problem, this paper proposes a novel *Quorum Rendezvous Channel Hopping (QRCH)* scheme [1]. Nodes are able to hop over random channels independently, bypassing the need for pre-key establishment. Furthermore, by using a quorum system, nodes are guaranteed to meet within a bounded time to exchange pending messages. The scheme also enables nodes to transmit packets to multiple receivers simultaneously. We validate the proposed scheme via extensive simulations and present its robustness and efficiency.**

I. Introduction

As wireless networks have been progressively more affordable and ubiquitous, providing security has become a critical concern. There is a security challenge unique to wireless networks which cannot be addressed by traditional solutions. For instance, a jamming attack could disrupt a wireless network; it is easily achieved by a malicious attacker (*jammer*) by injecting noise signals into the shared medium.

Utilizing spectral diversity such as Frequency-Hopping Spread Spectrum (FHSS) has been intensively investigated to cope with jamming attacks. Pseudo-random Channel (=Frequency) Hopping (PCH) is one of the promising countermeasures, which allows a pair of nodes to hop over multiple channels along a pre-shared random hopping sequence. Randomness of the sequence, unknown to jammers, ensures communications robust against jamming attacks. Yet, PCH requires the prior exchange of sequence information, namely pre-key establishment, before data transmission, which introduces critical constraints. First, this raises another issue of how to establish the initial secure key pairing containing the sequence data. Second, completing the key establishment phase takes nontrivial time; tens of seconds in the worst case [12]. Finally, PCH only supports one-to-one unicast since the key pairing is established exclusively between two nodes.

To overcome these limitations, this paper proposes a *Quorum Rendezvous Channel Hopping (QRCH)* scheme against jamming attacks using a quorum system. Unlike PCH, a sender and a receiver do not explicitly establish an initial key pairing. Instead, they start hopping over multiple random channels to transmit data from the very beginning, without having to rely on opportunistic encounters. The hopping sequences are constructed from a quorum system, which guarantees the nodes to meet within a bounded amount of time.

The major contributions of the paper are as follows: First, QRCH does not require any explicit pre-key establishment. By eliminating the initial key pairing phase, the scheme could achieve fast and resilient communication. Second, the quorum system ensures any pair of nodes to have at least one common element. Thus, the nodes in QRCH are more likely to rendezvous within a bounded time while they hop over multiple channels independently. Third, we introduce a new quorum-channel mapping strategy in the quorum-based channel hopping scheme. Finally, this is the first work that uses quorum for rendezvous in a hostile, jamming environment. All previous applications (e.g., spectrum reuse, etc) consider aggressive, but not malicious and hostile competitors.

The rest of the paper is organized as follows. In Section II, we review the jamming attack and its countermeasures. Section III gives a brief overview of the quorum system. Section IV presents the proposed QRCH scheme. In Section V, the proposed scheme is evaluated with simulation results. Finally, we conclude the paper in Section VI.

II. Jamming Attack

In a jamming attack, unlike conventional security threats, a jammer could disrupt a wireless medium by simply injecting false messages into the network. The shared nature of the wireless medium even empowers the jammer to disable all data transmissions within the radio range. In this sense, the jamming attack is regarded as a wireless version of Denial-of-Service (DoS). Gummadi *et al*. [3] investigated its impact on 802.11 networks. Noubir and Lin [10] observed that a power-constrained jammer can corrupt a small number of data bits, which leads to the loss of the entire packet. A jammer can disregard a MAC protocol: preventing nodes from commencing legitimate MAC operations or causing packet collisions [6]. The Australian CERT [1] showed the weakness of MAC protocol against a jamming attack in 802.11 networks. A jammer can also block data transmission by continuously injecting noise-like signals (or dummy packets) into a wireless

[1]The initial version of the paper was appeared in the poster session of ACM MobiCom 2010 [7].

978-1-4244-9229-9/10/$26.00 ©2010 IEEE

channel, namely a PHY-layer attack [15]. This work considers PHY-layer attacks; both internal and external jammers which are discussed in Section IV.

A. Countermeasure

Recently, channel hopping has attracted researchers' attention as a countermeasure against jamming attacks. Wood *et al.* [13] proposed *DEEJAM*, an anti-jamming scheme for Wireless Sensor Network (WSN) using PCH. Navda *et al.* [9] explored a proactive channel hopping scheme in which nodes hop over multiple channels regardless of the existence of jammers. Khattab *et al.* Gummadi *et al.* [3] proposed a rapid channel hopping scheme in which a node occupies a channel for a short period of time, i.e., $10ms$, with $250\mu s$ channel switching latency.

However, all of these PCH-based schemes require an extra pre-key establishment phase during which nodes share a common key, which introduces nontrivial constraints. First, the nodes must securely establish the initial key pairing. This requirement creates a circular dependency between anti-jamming channel hopping and key establishment [12]. Uncoordinated Frequency Hopping (UFH) [11], a secure pre-key establishment scheme, exploits a random frequency hopping technique inspired by Bluetooth. Before initiating communication, a sender and a receiver randomly switch over multiple frequencies. Upon meeting on the same frequency by chance, they exchange the common key. To increase the probability of encounters, nodes have different hopping speeds: the sender hops much faster than the receiver. In Bluetooth, a master hops around 20 times faster than a slave. Second, the key establishment phase takes considerable time. It is reported that Bluetooth takes $5.12s$∼$10.24s$ [4], and completing key establishment in UFH takes almost $40s$ when the jammer's attack probability is 60%. Whenever a communication link is crashed by a jamming attack, the nodes must resume key establishment phase, causing a huge latency overhead. Third, PCH is vulnerable to internal attackers. If a jammer becomes aware of the sequence information, then no communication would succeed due to jamming attack on all the visiting channels. Finally, PCH only considers one-to-one unicast. It allows a pair of nodes to establish a key pairing. A sender must make individual key establishment to all neighbors to achieve broadcast communications, causing a scalability problem.

III. Quorum System

This section provides a brief definition of a quorum system and describes its two fundamental properties; *intersection property* and *rotation closure property*. For definitions, we borrow terminologies from [5, 8].

A. Definition and Property

Definition 1. Given a finite universal set $U = \mathbb{Z}_N = \{0, 1, ..., N-1\}$ of *N* elements, a *quorum system Q* under *U* is a collection of non-empty subsets of *U*, which satisfies the *intersection property*:

$$\forall G, H \in Q;\ G \cap H \neq \emptyset.$$

Each G or $H \in Q$ is called a *quorum*, and $\mathbb{Z}_N$ represents a set of non-negative integers less than *n*.

Definition 2. Given a non-negative integer i and a quorum H in a quorum system Q under $U = \{0, ..., N-1\}$, we define:

$$rotate(H, i) = \{(h + i) \bmod N \mid h \in H\}.$$

Definition 3. A quorum system Q under $U = \{0, ..., N-1\}$ has the *rotation closure property* if the following holds:

$$\forall G, H \in Q \text{ and } i \ \in \{0, ..., N-1\};\ G \cap rotate(H, i) \neq \emptyset.$$

For example, a quorum system $Q = \{\{0,1\}, \{0,2\}, \{1,2\}\}$ under $U = \mathbb{Z}_3 = \{0,1,2\}$ has the rotation closure property. On the other hand, $Q' = \{\{0,1\}, \{0,2\}, \{0,3\}\}$ under $U' = \mathbb{Z}_4 = \{0,1,2,3\}$ has no the rotation closure property.

All quorum systems hold the intersection property. Yet, some of them satisfy the rotation closure property. In particular, the proposed QRCH exploits a *cyclic quorum system* [8] to construct a set of hopping sequences, which is reviewed in the following subsection.

B. Cyclic Quorum System

Definition 4. A subset $D = \{a_1, ..., a_\kappa\} \subset \mathbb{Z}_N,\ a_i \in \{0, ..., N-1\}$ and $\kappa \leq N$, is called a *cyclic* (N, κ) *difference set* if for every $d \not\equiv 0 \pmod N$ there exist at least one pair of elements (a_i, a_j) such that $a_i - a_j \equiv d \pmod N$.

Given any *N*, Jiang *et al.* [5] proved that $\sqrt{N} \leq \kappa \leq N$. When selecting the minimum κ, we call it a *minimal (N,κ) difference set*.

Definition 5. Given a (N, κ) difference set $D = \{a_1, ..., a_\kappa\} \subset \mathbb{Z}_N$, a *cyclic quorum system constructed by D* is $Q = \{G_0, ..., G_{N-1}\}$, where $G_i = \{a_1 + i, a_2 + i, ..., a_\kappa + i\} \pmod N$ and $i = 0, ..., N-1$.

For a (7,3) difference set $D = \{0,1,3\} \subset \mathbb{Z}_7$, for instance, the set $\{0,1,3\}$ modulo 7 yields $d = \{1, ..., 6\}$. Then, a cyclic quorum system $Q = \{G_0 = \{0,1,3\}, ..., G_6 = \{6,0,2\}\}$ is constructed from D.

IV. Quorum Rendezvous Channel Hopping

This section presents our novel *Quorum Rendezvous Channel Hopping (QRCH)* scheme. We discuss on design of a channel hopping system and describe our system.

A. Problem Definition

Suppose that we are given *N* available channels in a wireless network and time is divided into channel hopping periods each of which is composed of *t* time slots. Constructing a channel hopping system is a process of assigning channels to all time slots and determining a channel hopping sequence, *X*, denoted:

$$X = \{x_0, ..., x_t\} = \{(0, c_0), ..., (t-1, c_{t-1})\},$$

where $x_i \in X$ contains a tuple of (*time slot index*, *channel index*) and $c_i \in \{0, ..., N-1\}$ represents the channel index at time slot *i* in a period. Given two channel hopping sequences *X* and *Y*, they are said to *rendezvous* if they have at least one element in common; $x_i = y_i\ (0 \leq i \leq t-1)$. If a pair of

nodes selects the sequences of *X* and *Y* respectively, then they are guaranteed to be on the same channel at the same time at least once within a period.

B. Quorum Rendezvous Channel Hopping

Algorithm 1 QRCH System Construction Algorithm

Require: $N, \kappa, U = \mathbb{Z}_N$, and a cyclic quorum system Q
Ensure: Sending sequence X and receiving sequence Y
1: Select i randomly, where $i \in U = \{0, ...N-1\}$
2: Obtain a quorum $G_i = \{g_0, ..., g_{\kappa-1}\}$, where $G_i \in Q = \{G_0, ..., G_{N-1}\}$
3: $X = \emptyset$ and $Y = \emptyset$
4: **for** $j = 0$ to $\kappa^2 - 1$ **do**
5: $\quad m \leftarrow j \bmod \kappa$
6: $\quad n \leftarrow (j - (j \bmod \kappa))/\kappa$
7: $\quad x_j = (j, g_m)$, where $g_m \in G_i$
8: $\quad y_j = (j, g_n)$, where $g_n \in G_i$
9: $\quad X \leftarrow X \cup x_j$
10: $\quad Y \leftarrow Y \cup y_j$
11: **end for**
12: **return** $X = \{x_0, ..., x_{\kappa^2-1}\}$ and
13: $Y = \{y_0, ..., y_{\kappa^2-1}\}$

Algorithm 1 constructs the QRCH system by assigning channels to time slots. We present the algorithm with an example by setting $N = 7$ and $\kappa = 3$, a *minimal (N,κ) difference set*. The following procedure explains it.

1) Construct a universal set $U = \mathbb{Z}_7 = \{0, ..., 6\}$ and determine a (7,3) difference set D, ($\sqrt{7} \leq 3 \leq 7$).
2) Construct a cyclic quorum system $Q = \{G_0, ..., G_6\}$ from D.
3) A node *A* selects a random number *1* from U, and then obtains a quorum $G_1 = \{1, 2, 4\}$ from Q.
4) The following equation assigns a channel to the time slot *j* using the quorum $G_1 = \{1, 2, 4\}$.
$$x_j = (j, g_m) \text{ and } y_j = (j, g_n)$$
where $m = j \bmod \kappa$ and $n = (j - (j \bmod \kappa))/\kappa$.
5) Repeat step (4) for all 9 (= κ^2) time slots. This constructs a sending sequence $X = \{(0,1), (1,2), (2,4), (3,1), (4,2), (5,4), (6,1), (7,2), (8,4)\}$ and a receiving sequence $Y = \{(0,1), (1,1), (2,1), (3,2), (4,2), (5,2), (6,4), (7,4), (8,4)\}$.
6) A node *B* repeats step (4-5) with a selected quorum $G_3 = \{3, 4, 6\}$, and then, construct two hopping sequences X' and Y'.

Figure 1 illustrates rendezvous at the QRCH system when the nodes *A* and *B* choose the sequence X and Y', respectively. As shown, they rendezvous on *channel 4* at *time slot 5*.

While sitting on a channel, a sender (*A*) periodically broadcasts HELLO messages. When a receiver (*B*) hears the message, it replies with a HELLO ACK message. Then, *A* starts transmitting data packets to *B*. During HELLO message exchange, the nodes could authenticate each other and synchronize their hopping sequence for further data transmission.

		One time period								
		Frame 1			Frame 2			Frame 3		
	Time slot	0	1	2	3	4	5	6	7	8
A takes X	Quorum G_1	1	2	4	1	2	***4***	1	2	4
B takes Y′	Quorum G_3	3	3	3	4	4	***4***	6	6	6

Fig. 1. QRCH with (7,3) difference set under $\mathbb{Z}_7$. The node *A*, as a sender, uses the sending sequence X, and the node *B* uses the receiving sequence Y'. They rendezvous on *channel 4* at *time slot 5*.

QRCH has three distinctive characteristics. First, QRCH exploits a *quorum-channel mapping* strategy. The elements in a selected quorum are mapped into channel indexes. For example, when a quorum $G_1 = \{1, 2, 4\}$ is selected, a node assigns channels 1, 2, and 4 from $\mathbb{Z}_7$ to consecutive time slots. Second, after selecting a quorum randomly, a node generates two different channel hopping sequences: a *sending sequence* and a *receiving sequence*. If a node has data to transmit, it hops channels according to the *sending sequence*. Otherwise, the node follows the *receiving sequence*. Last, the quorum size determines the length of one time period. Say, given quorum size κ, one period consists of $|\kappa|$ frames each of which contains $|\kappa|$ time slots. In short, the length of one time period = κ^2 time slots. The length of the period indicates upper bound since QRCH guarantees at least one rendezvous within one period when there is no jammer. To build a hopping sequence, QRCH makes use of the *minimal* (N, κ) *difference set* where κ approximates its lower bound $\sqrt{N}$. Thus, the upper bound of time cost for rendezvous in QRCH, κ^2, also approximates N which is the optimal value on channel hopping given N channels. Recall that all other existing schemes provide no upper bound.

C. Robustness

This paper considers PHY-layer attacks, and it is of the utmost concern to know how robust QRCH is against various jamming attacks.

First, suppose an active external jammer, namely *Continuous-Random (CR) jammer*. For each time slot, the jammer randomly chooses a target channel on which it jams. Then, it jumps to another random channel to attack without any pause. The CR jammer repeats this jamming process. The probability of successful attack relies on jammer's channel selection on a time slot, which is $\frac{1}{N}$. This probability is same to that of RH.

Second, a passive *Intelligent (IT) jammer* initially monitors ongoing transmissions on a randomly selected channel and launches an attack only when a signal has been detected. The probability of successful attack relies on the dwell time during which a node stays on a channel. As Gummadi mentioned in [3], a fast channel hopping (i.e., $10ms$ of dwell time) can avoid the IT jammer since jamming detection can take up to several seconds [15] and $10ms$ is not enough time to detect transmission and to start jamming. Furthermore, channel switching latency reduces down to tens of micro-seconds [2], which makes the fast channel hopping more attractive.

Last, a responsive *Internal (IN) jammer* is aware of the

quorum parameters used in communication. It constructs own random hopping sequence from (N, κ) difference set and listens to a sender; impersonating a legitimate receiver. When rendezvous with the sender, the jammer tries to establish a fake connection, which causes a failure of legitimate communication. Fortunately, however, the IN jammer could be eventually detected via an authentication process such as Diffie-Hellman key establishment protocol [14]. Nonetheless, the attack could still happen up to 50% of the times, which causes the waste of time slots and thus delayed rendezvous.

V. Evaluation

A. Preliminary

The QRCH system is implemented on MATLAB. It exploits the cyclic quorum system using minimal (N, κ) difference sets [8]. For performance comparison, we implement PCH[2] and Random Hopping (RH) in which a sender and a receiver hop over random channels independently (with same hopping speed). Our experiments use the CR jammer as a default jamming attack model as well as the IN jammer. With respect to an authentication process, we assume using Diffie-Hellman key establishment protocol [14] and $10ms$ of channel dwelling time in IEEE 802.11a. Then, the sender could complete the authentication within one time slot. Our experiment assumes the worst case of overhead in which the sender wastes the entire one time slot when it rendezvous with the IN jammer. In a network, there is one sender, receiver, and jammer by default, and we report results by averaging the outputs from 1000 simulations.

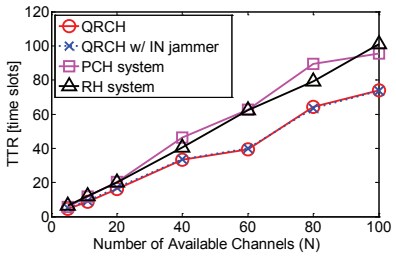
Experiments measure three metrics. Time-To-Rendezvous (TTR) is an average time for nodes to rendezvous. Rendezvous Probability (RP) indicates possibility of successful rendezvous among nodes. Probability of Successful Attack (PSA) represents the efficiency of a jamming attack. We count the number of successful jamming out of total number of rendezvous.

B. Experiments and Results

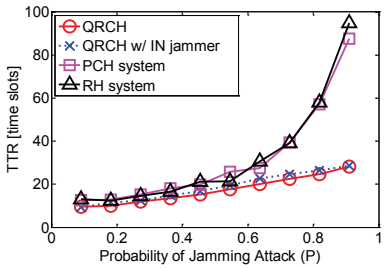
1) Impact of channels and jammers: In the first experiment, we vary the number of available channels (*N*) from 5 to 100. As shown in Figure 2(a), QRCH shows a lower TTR than those of PCH and RH, which indicates that a sender rendezvous with a receiver quickly. The gaps become clear as *N* increases because nodes in PCH and RH randomly select channels out of the increasing number of channels. The plot also tells that QRCH is very robust against one IN jammer so that it maintains good shape of TTR values. Yet, it is necessary to scrutinize packet overheads due to the fake connection request by the IN jammer, which is one of our future work.

The next experiment increases the number of jammers from 1 to 10 in a wireless network having 11 potential channels. Jammers are assumed to collude with each other, so no two jammers attack the same channel simultaneously. Having 10 jammers implies that 10 channels are jammed out of 11, which computes jamming probability (*P*) of 91%. Then, nodes can

[2]A sender hops channels 20 times faster than a receiver like Bluetooth



(a) Impact of varying number of available channels (N).



(b) Impact of varying number of jammers (P).

Fig. 2. Time-To-Rendezvous performance.

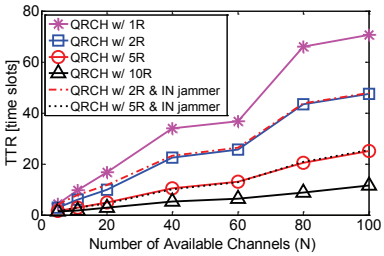
only transmit packets through the single remaining channel. PCH and PH show TTRs increasing as *P* increases in Figure 2(b). On the contrary, QRCH displays robustness against various *P*. In particular, QRCH maintains good performance even when *P* = 91%: 29 TTR compared to 94 TTR in RH. Due to the upperbound of κ^2 TTR, QRCH could keep lowering TTR in the presence of heavy jamming.

2) Impact of varying number of receivers: QRCH is evaluated with varying numbers of receivers (*R*). For instance, 5*R* represents 5 receivers in the sender's radio range. The experiments also have varying number of *N*, and the results are depicted in Figure 3. There is still one sender and one jammer in the experiments.

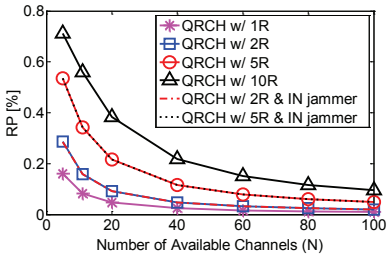
Figure 3(a) shows that the more the number of *R*, the better TTR performance of QRCH. Even with *N* of 100, 5 receivers achieve around 20 time slots of TTR. This implies that neighboring nodes in a dense network could cooperate to mitigate jamming attacks. A multi-path routing could be investigated to exploit this observation. Two dotted curves, almost overlapped with other lines, illustrate TTR performance with the presence of the *IN* jammer in which QRCH still provides excellent performance.

Performance of RP is shown in Figure 3(b). Given multiple receivers, RP represents one-hop packet delivery ratio. In the experiment, we count one delivery if at least one receiver rendezvous. Having higher *R* results in better performance. When using 5 channels with 10*R*, the ratio goes over 70%, which means that 7 packets out 10 are delivered successfully to one-hop neighbors under a jamming attack. The figure also shows that QRCH is robust against the IN jammer.

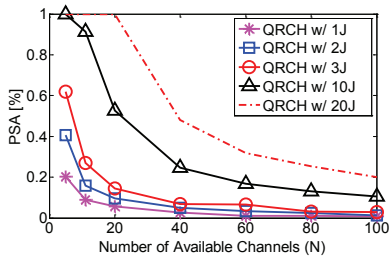
In the last experiment, we increase the number of the IN jammers (*J*) while still varying *N*, and then measure PSA.



(a) Time-To-Rendezvous (TTR) performance. *R* stands for receiver; *5R* represents 5 receivers.



(b) Rendezvous-Prob. (RP) performance.



(c) Prob.-of-Successful-Attack (PSA) performance. *10J* represents 10 IN jammers.

Fig. 3. Performance of QRCH with varying number of receivers (R).

The experiment has one receiver. Three colluded IN jammers achieve 27% of PSA when using 11 channels (see the circular mark in 3(c)). This means that 27 time slots are jammed given 100 rendezvous slots. PSA decreases rapidly as N increases, so that PSA drops below 10% when 30 channels are available. This suggests that increasing N can significantly mitigate the effects of a jamming attack.

VI. Conclusion

We have proposed a novel *Quorum Rendezvous Channel Hopping (QRCH)* scheme that makes wireless communication more robust against jamming attacks. QRCH allows nodes to hop over multiple channels along the hopping sequences selected independently and randomly. Using a quorum system guarantees the nodes to meet within a bounded time. QRCH does not explicitly require any initial key establishment, henceforth, it could easily scale up. The experiments show that the proposed scheme outperforms existing methods under various jamming attack models. The study of QRCH on designing a reliable wireless multi-hop routing protocol will be an integral part of our future work.

References

[1] Auscert. aa-2004.02 - denial of service vulnerability in ieee 802.11 wireless devices. http://www.auscert.org/.

[2] P. Bahl, R. Chandra, and J. Dunagan. Ssch: slotted seeded channel hopping for capacity improvement in ieee 802.11 ad-hoc wireless networks. In *ACM MobiCom*, 2004.

[3] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan. Understanding and mitigating the impact of rf interference on 802.11. In *ACM Sigcomm*, 2007.

[4] E. Hall, D. Vawdrey, and C. Knutson. Rf rendez-blue: reducing power and inquiry costs in bluetooth-enabled mobile systems. In *IEEE ICCCN*, Oct. 2002.

[5] 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. In *ACM Mobile Networks and Applications*, 2005.

[6] Y. W. Law, P. Hartel, J. den Hartog, and P. Havinga. Link-layer jamming attacks on s-mac. In *European Workshop on Wireless Sensor Networks (EWSN)*, 2005.

[7] E.-K. Lee, S. Y. Oh, and M. Gerla. Frequency quorum rendezvous for fast and resilient key establishment under jamming attack. In *ACM MobiCom Poster*, Chicago, USA, Sep. 2010.

[8] W.-S. Luk and T.-T. Wong. Two new quorum based algorithms for distributed mutual exclusion. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 1997.

[9] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein. Using channel hopping to increase 802.11 resilience to jamming attacks. In *IEEE Infocom*, 2007.

[10] G. Noubir and G. Lin. Low-power dos attacks in data wireless lans and countermeasures. *ACM Mobile Computing and Communications Review*, 7(3):29–30, 2003.

[11] M. Strasser, C. Popper, and S. Capkun. Efficient uncoordinated fhss anti-jamming communication. In *ACM MobiHoc*, 2009.

[12] M. Strasser, C. Popper, S. Capkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In *IEEE Symposium on Security and Privacy*, 2008.

[13] A. Wood, J. Stankovic, and G. Zhou. Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks. In *IEEE SECON*, 2007.

[14] A. X9.63-2001. Key agreement and key transport using elliptical curve cryptography. Technical report, American National Standards Institute, 2001.

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *ACM MobiHoc*, 2005.