SPREAD: Foiling Smart Jammers using Multi-layer Agility

Xin Liu, Guevara Noubir, Ravi Sundaram, San Tan
College of Computer and Information Science
Northeastern University, Boston, MA 02115
{liux, noubir, koods, tansan} @ ccs.neu.edu

***Abstract*— In this paper, we address the problem of cross-layer denial of service attack in wireless data networks. We introduce SPREAD - a novel adaptive diversification approach to provide resiliency against such attacks. SPREAD relies on a mechanism-hopping technique, which can be seen as a multi-layer extension of the frequency-hopping technique. We apply a game-theoretic framework for modeling the interaction of the communicating nodes and the adversaries and analyze the proposed approach. We reason about the advantages of SPREAD against various types of jammers and demonstrate the effectiveness of our approach in the case of IEEE 802.11 protocol stack by studying the EIFS attack, periodical jamming and a Packet-Size Game. As an example, we show that mechanism-hopping over two instances of IEEE 802.11 can achieve several orders of magnitude gain in throughput over a single-instance network under the EIFS attack.**

I. Introduction

Wireless networks are highly sensitive to Denial of Service (DoS) attacks [1], [2]. The wireless communication medium is a broadcast channel, exposing the physical layer of wireless communication to jamming. Past research has mostly focused on defending voice communication using spread spectrum techniques [3]. Such approach spreads the signal into a very large frequency band and makes a jammer with limited energy resources unable to afford jamming the entire band. Noncontinuous jamming only results in a graceful degradation of the voice quality. Therefore, the approach is effective to protect voice communication against jamming.

Earlier the wireless traffic used to be monotonous, but recently there has been a wide diversification in the nature of wireless traffic and the corresponding network architectures. A jammer can be very smart and cause DoS efficiently by launching cross-layer attacks. For instance, a jammer can monopolize the communication medium by exploiting the carrier sensing mechanism at MAC layer of communication nodes [4], [5]. The jammer sending short interfering pulses periodically can make other nodes in the vicinity feel the medium is always busy and defer the transmissions. Or the jammer can exhaust the energy of communication nodes by destroying the acknowledgement packets and forcing the communication nodes to continuously retransmit the packet [5], [6]. In [7], we have shown that there exists an efficient jamming attack against wireless data networks which consumes 10^4 less energy than continuous jamming. The control mechanisms of the routing protocols are essential for the functionality and, therefore, are also targets of smart jamming [8], [9]. By destroying the route discovery or neighbor discovery packets, a jammer can disconnect the network. The vulnerability is further aggravated in the case of mobile multi-hop networks due to their dynamic-topology characteristic, which requires frequent route discovery and adjustment.

The single protocol-stack in existing systems makes very efficient smart jamming possible. If the adversary knows the specific mechanism at each layer, it can cripple the network by attacking the critical bits or phases at a carefully chosen moment and location. The Wolfpack program of DARPA in particular has focused on developing attacks that sense the protocol suite in use, and then tailor the attack to the specifics of that suite [1], [10].

In this paper, we introduce a novel approach called SPREAD (Second-generation Protocol Resiliency Enabled by Adaptive Diversification) to provide resiliency to adversaries in heterogeneous wireless networks. The key idea of SPREAD is to avoid having any single focal point or failure bottleneck by providing a well-chosen collection of parallel networking stacks and switching between mechanisms dynamically. From a conceptual perspective, SPREAD puts the interaction between the communicating nodes, and jammers in the framework of game theory. Each player, the communication nodes and the jammer, has a collection of strategies and different objectives. Game theory, which originated in the field of economics used as a tool to describe market dynamics [11], has been widely used from nuclear deterrence to communications in recent years [12], [13]. To the best of our knowledge, this is the first time it is used in a cross-layer jamming setting. From a protocol perspective, SPREAD relies on a novel mechanism-hopping technique. Based on the observation that smart attacks against one communication mechanism may not be efficient against another, SPREAD prevents the adversary from attacking a known weak point by cryptographically hopping between multiple mechanisms. Recently, we have investigated the problem of synchronized protocols switching in the context of network virtualization. We showed that it is feasible to implement it on linux-based computers with switching order of a few hundreds of milliseconds [14]. We believe that switching in the order of a sub-millisecond is feasible but requires dedicated hardware.

Our Contributions: 1) we introduce a novel approach, SPREAD, to combat smart jamming attacks against wireless data networks; 2) we use a game theoretical framework to

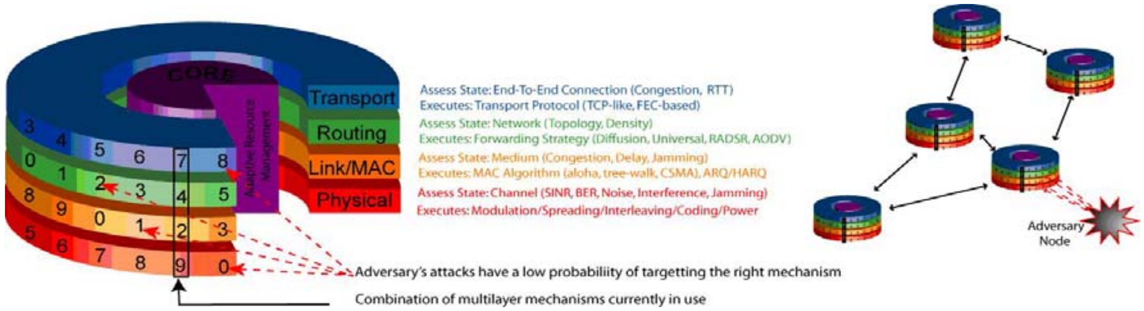
CORE
Adaptive Resource Management
3 4 5 6 7 8
0 1 2 3 4 5
8 9 0 1 2 3
5 6 7 8 9 0
Transport
Routing
Link/MAC
Physical
Assess State: End-To-End Connection (Congestion, RTT)
Executes: Transport Protocol (TCP-like, FEC-based)
Assess State: Network (Topology, Density)
Executes: Forwarding Strategy (Diffusion, Universal, RADSR, AODV)
Assess State: Medium (Congestion, Delay, Jamming)
Executes: MAC Algorithm (aloha, tree-walk, CSMA), ARQ/HARQ
Assess State: Channel (SINR, BER, Noise, Interference, Jamming)
Executes: Modulation/Spreading/Interleaving/Coding/Power
Adversary's attacks have a low probabiliity of targetting the right mechanism
Combination of multilayer mechanisms currently in use
Adversary Node

Fig. 1. The cylinder principle and mechanism-hopping of SPREAD. Each layer has multiple protocols.

model the communicating nodes and jammers as rational players in a noncooperative game with different objectives; and 3) we demonstrate the effectiveness of our approach against adversaries in the case of IEEE 802.11. SPREAD greatly increases the network robustness against smart attacks such as the EIFS attack.

II. The Approach

SPREAD consists of two parts, the cylinder architecture and mechanism-hopping.

A. Cylinder Architecture

The cylinder architecture supports multiple protocols per layer and allows an efficient control of the layers through the CORE. Figure 1 illustrates the cylinder architecture.

The CORE: The CORE constitutes the brain of the communication system. It collects status information from each layer (e.g., channel state, SNR, energy, network congestion), and makes decisions on mechanisms and parameter values used at each layer based on the available resources (i.e., energy, radio frequency bandwidth, channel state, application requirements, interference and adversarial activity). The CORE cryptographically generates the hopping sequence and takes care of hopping synchronization over multiple mechanisms.

Layers: Each layer provides implementation of multiple mechanisms. Our architecture falls in between a completely unstructured communication system and the traditional layered system. It retains the advantage of a layered approach by providing the implementation of functionalities within each layer while leaving the control and coordination to the CORE. The functionalities of each layer within the context of the SPREAD approach are described as follows.

- **Physical Layer:** the physical layer provides the CORE with accurate channel assessments including the received signal strength, noise level, and interference level. The CORE decides, on a per-packet basis, the value of the following parameters: spreading factor, power level, modulation, coding, share of MIMO streams, channel, time slot, etc.
- **Medium Access Control Sub-Layer:** the MAC layer implements the details of the access control mechanism, e.g., aloha, CSMA/CA, TDMA. The CORE makes decisions about the specific mechanism and its parameters, e.g., back-off coefficient, p-persistency, priority.
- **Data Link Control Sub-Layer:** this layer implements various data link control mechanisms, including ARQ (Go-Back-N, Selective-Repeat), Hybrid-ARQ (types I, II, and III), and unreliable link control. The CORE makes decisions based on the tradeoffs of delay, reliability, and robustness against adversaries.
- **Routing Layer:** in this layer, multiple strategies for forwarding packets to the destination can be used, e.g., DSR, AODV, SAODV, ARIADNE. The CORE makes choices based on the susceptibility level to the adversaries, delay, overhead, mobility, and etc.

B. Mechanism-hopping

Nodes switch between mechanisms throughout the communication. The mechanism-hopping patterns are controlled by the CORE and are negotiated between single-hop and multi-hop peers. The pseudorandom hopping sequence prevents a smart jammer from easily identifying the critical point at a given instant of time. A random guess of the mechanism in use gives a jammer a low chance of success. We define two types of mechanism-hopping techniques:

- **Inter-protocol mechanism-hopping:** in this case, multiple physical protocols run in an interleaved mode, each has an independent state machine. We also identify *multi-instance* mechanism-hopping as interleaving of multiple instances of one protocol, each with its own state.
- **Intra-protocol mechanism-hopping:** in this case, a single protocol is running but cryptographically hops between parameters such as packet size, coding rate, and interleaving scheme.

Depending on the available resources on the communication nodes and jamming strategies, the CORE determines which mechanism-hopping strategy should be used.

III. The Case of Single-hop IEEE 802.11

In this section, we demonstrate the effectiveness of SPREAD in the case of an IEEE 802.11 network. First, we show how mechanism-hopping over two IEEE 802.11 instances mitigates a denial of medium access attack, EIFS attack. Then, we describe the potential of SPREAD through an example of intra-protocol mechanism-hopping that increases the network resiliency to periodical jamming.

A. SPREAD Against the EIFS Attack

The EIFS Attack: IEEE 802.11 requires nodes to sense the medium before transmission. A wireless node has to defer the transmission until the medium has been idle without interruption for a period of DIFS (DCF Interframe Space) or EIFS (Extended Interframe Space) [15]. If the last frame reception is successful, DIFS is applied. Otherwise, EIFS must be applied. For IEEE 802.11 DSSS (Direct Sequence Spread Spectrum), DIFS is 50 μs, and $EIFS$ is 364 μs.

A serious vulnerability of IEEE 802.11 arises from the requirement of carrier sensing for $EIFS$ whenever the physical layer notifies the MAC layer of a reception failure. A jammer can monopolize the channel by sending out a noise-like jamming pulse before the end of every EIFS. This forces the communication nodes to stay in the waiting (for EIFS) state forever. As a result, the jammer blocks the communication nodes from initiating a transmission. We name this attack EIFS attack, and verify the attack through simulation. As shown in Figure 3, the IEEE 802.11 throughput is zero under the EIFS attack. The original form of this medium access attack against IEEE 802.11 is SIFS attack which was discovered in [4]. The EIFS attack is much more energy efficient for the jammer than the SIFS attack since the EIFS is 35 times longer than the SIFS, which is 10 μs in IEEE 802.11 DSSS.

Mechanism-hopping Counterattacks EIFS Attack: SPREAD can help mitigate the attack by introducing one more IEEE 802.11 instance to the sender and the receiver. The two instances, denoted as 802.11-I and 802.11-II, are equiprobably scheduled in a TDM manner . The length of a time slot is $\frac{EIFS}{2}$. Figure 2 illustrates mechanism-hopping over 802.11-I and 802.11-II. The randomness introduced by mechanism-hopping prevents the EIFS jammer from hitting one instance all the time; therefore, the IEEE 802.11 throughput is higher than zero.

Figure 3 shows the simulation result using Qualnet3.9 [16]. IEEE 802.11 operates at 11 Mbps. The traffic is CBR with a packet size of 400 bytes. The IEEE 802.11 throughput is 2.91 Mbps without jamming in the network, and it drops to zero under the EIFS attack. The third group of bars represents the throughputs of 802.11-I and 802.11-II of SPREAD without jamming in the network. Each gets 1.45 Mbps, an even share of the network throughput. The last group represents the throughputs of the two instances of SPREAD under the EIFS attack, which are 0.338 Mbps and 0.336 Mbps, respectively. Therefore, the SPREAD network has a total throughput much higher than that of a non-SPREAD network.

B. SPREAD Against Periodical Jamming

In this section, we use an example to demonstrate the potential of SPREAD foiling smart jamming attacks by deploying intra-protocol mechanism-hopping. The intra-protocol mechanism-hopping adds diversity to the network such that a smart jammer with a single jamming scheme becomes much less effective in a SPREAD network.

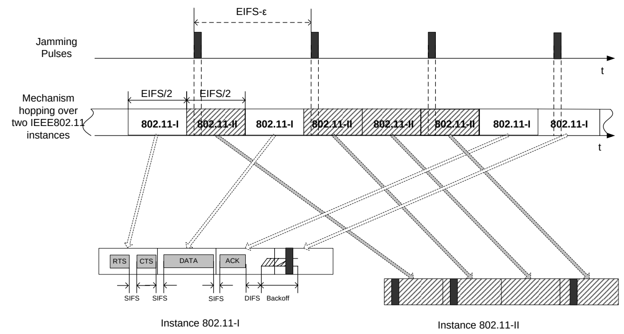

Fig. 2. Mechanism-hopping over two instances of IEEE 802.11.

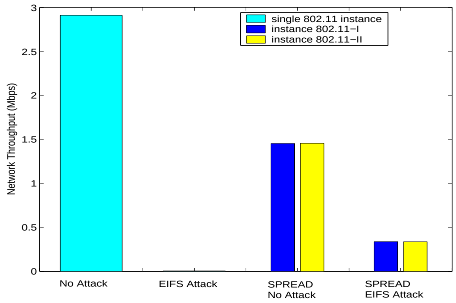

Fig. 3. Simulation of IEEE 802.11 throughout with and without EIFS attack. Throughput of each instance of mechanism-hopping with and without EIFS attack.

First, we show that a smart periodical jammer can interrupt a single instance of IEEE 802.11 effectively. Consider a setup with two communication nodes and a periodical jammer, which sends jamming pulses at a fixed rate with fixed pulse width. The jammer is located close to the receiver. It can affect the receiver but not the sender. The data rate in use is 1 Mbps. Unlike IEEE 802.11a, IEEE 802.11b does not use an error-correction scheme at the physical layer. Therefore, a single jamming pulse with width of 1 bit is able to destroy a large data packet (e.g. 1500 bytes) [7]. Consider two instances of IEEE 802.11b traffic. One, denoted as 802.11-SP, has a packet size of 100 bytes. The other, denoted as 802.11-LP, has a packet size of 1530 bytes. Since it is expensive to lose a large packet, RS(255,233) error control coding is applied to 802.11-LP to protect the data packets [17]. Without jamming, each traffic alone gets a throughput of 211 Kbps and 782.7 Kbps respectively. Consider a jammer, Jammer-SP, sends out short jamming pulses at a rate close to the data rate of 802.11-SP, to attack 802.11-SP traffic. Since the 802.11-SP data packet does not have error-correction protection, the narrow jamming pulse is sufficient to destroy the data reception at the receiver. The throughput of 802.11-SP drops to 631 bps under this jamming. Consider another jammer, Jammer-LP, sends wide jamming pulses that exceed the error-correction capability of the RS code at a rate close to the data rate of 802.11-LP to jam 802.11-LP traffic. The throughput of 802.11-LP decreases to 4849 bps under Jammer-LP attack.

TABLE I

NETWORK THROUGHPUTS UNDER DIFFERENT JAMMING SCHEMES

	802.11-SP	802.11-LP	Intra-protocol hopping
No Jammer	211 Kbps	782.7 Kbps	
Jammer-SP	631 bps	782.7 Kbps	394.9 Kbps
Jammer-LP	187 Kbps	4849 bps	106.8 Kbps

As we see, if the IEEE 802.11 nodes use a unique communication scheme, a smart jammer can find a jamming scheme that dramatically reduces the throughput. Now we show that the SPREAD approach greatly enhances the network robustness against a jammer with a single jamming scheme. SPREAD applies intra-protocol mechanism-hopping over 802.11-SP and 802.11-LP in this example. The mechanism-hopping schedules the two instances at each slot equiprobably. Table I shows that if the jammer launches Jammer-SP attack, SPREAD achieves a throughput of 394.9 Kbps which is 624 times higher than what 802.11-SP gets. If the jammer launches Jammer-LP to attack SPREAD, SPREAD achieves a throughput of 106.8 Kbps, which is 21 times higher than what 802.11-LP gets. Although Jammer-SP is effective to destroy 802.11-SP, it could not impair 802.11-LP due to the error correction capability from the RS code. Jammer-LP is efficient to jam 802.11-LP, but its infrequent jamming pulses allow many 802.11-SP data packets to get through. Therefore, the coexistence of the two 802.11 schemes in SPREAD and the random mechanism-hopping over them makes the network more robust.

IV. SPREAD IN A PACKET-SIZE GAME

In SPREAD, the communication nodes can keep jammers guessing by cleverly changing the communication mechanisms. One might ask, what is the set of mechanisms that communication nodes should hop between and what fraction of time they should use each mechanism for? Is there any optimal operation point? In this section, we use a game theory framework to model SPREAD against jamming. Using a Packet-Size Game example, we describe how to determine the hopping strategies and qualify the benefit of SPREAD.

A. Game Theory

In game theory, each player has a set of possible actions which are known as pure strategies [11], and probability distributions over these pure strategies are known as mixed strategies. In 1950 Nash [18] proposed a fundamental concept in game theory which has since come to be known as Nash equilibrium. A Nash equilibrium is a point where no individual player can benefit from unilateral deviation. Nash equilibria are precisely what we are looking for because they represent stable operating points in SPREAD. If a point is not a Nash equilibrium then either the communication nodes or the jammer will change their strategy so as to improve their payoff. In his seminal paper [18], Nash proved that every finite game has a mixed Nash equilibrium. Furthermore, a Nash equilibrium automatically specifies the pure strategies (mechanisms) and the probability distribution over them. This answers the question of what mechanisms the hopping sequence should jump between and in what relative frequency. Although it has been proved that computing a mixed Nash equilibrium is computationally infeasible [19], we can utilize the concept of approximate Nash equilibria which are characterized by the property of having small support [20].

B. Packet-Size Game

To formulate and analyze the use of SPREAD to counter jamming with different coding schemes, packet sizes and energy constraints is very hard. As a first step, we study a relatively simpler interaction: Packet-Size Game, where the communication nodes can use multiple packet sizes and the jammer can use multiple jamming rates. Research has been done on using adaptive packet size to enhance throughput in wireless networks [21]. Our focus here is to use adaptive packet size schemes to counter jamming. The jammer could have more strategies than various jamming rates, but to simplify the analysis, we consider only different jamming rates in this paper. The tradeoffs in this game are: short packet traffic can survive jamming but results in more overhead and therefore smaller throughput; long packet traffic has less overhead therefore larger throughput but is easier to be jammed; the high rate jammer can reduce the throughput significantly, but it consumes more energy; the low rate jammer consumes less energy but misses many data packets.

Game Theoretical Formulation: This is a two-player noncooperative game. The participants are the communication nodes on one side and the jammer on the other side. The players are rational and make decisions independently based on their own interests. Denote player set as $P = (P_1, P_2)$, where P_1 is the communication nodes, and P_2 is the jammer.

The action set (or strategies) for the communication nodes includes a choice of different packet sizes. The action set for the jammer includes a choice of different jamming rates. Denote the action set as $A = A_1 \times A_2$, where $A_1 = (L_1, \ldots, L_n)$ is for P_1 and $A_2 = (R_1, \ldots, R_m)$ is for P_2.

Utility Functions: The utility function represents the objective of a player. For the communication nodes, three possible utility functions can be considered. The first utility function is THROUGHPUT. There is no limitation on energy. This makes sense for nodes with a replenishable source of energy. The second possible function is (THROUGHPUT/ENERGY). This ratio indicates the efficiency of the communication nodes in terms of bits transmitted per Joule. This makes sense for nodes with limited sources of energy (e.g., wireless sensor nodes). The third potential utility function is (THROUGHPUT - A*ENERGY) where A is a parameter of communication nodes specifying that they want to achieve the successful delivery of at least A bits per Joule but want to maximize beyond that threshold. Here, we use the first utility function assuming that the nodes energy sources can be replenished. Future research will address other scenarios and utility functions.

Similarly, two utility functions can be defined. The jammer is interested in how many bits it can prevent from being transmitted. The first possible utility function is (MAXTHROUGH-

PUT - THROUGHPUT) with a power bound. It makes sense for jammers without energy limitation. The second utility function is (MAXTHROUGHPUT - THROUGHPUT) - A*ENERGY, where A is the minimum amount of throughput-reduction the jammer expects when spending one unit of energy. The second utility function makes sense for jammers with a limited energy resource (e.g., cyber-mines). One can note that when $A = 0$ the jammer becomes a continuous jammer [3]. When $A = \infty$, the jammer will refrain from jamming. A is set by the adversary depending on his goal and the available energy resources. We use the second utility function in this paper. Denote the utility function set as $\{U\} = \{U_1, U_2\}$. We have $U_1 =$ THROUGHPUT and $U_2 =$ (MAXTHROUGHPUT - THROUGHPUT)-A*R,where R is the jamming rate, therefore representing the energy.

Since the Packet-Size game is a finite game, a mixed strategy equilibrium always exists [11]. Finding the Nash equilibrim of two-player game is proved to be a PPAD-complete problem in [19]. The difficulty of the problem lies in determining the support. Given the support set, the Nash equilibrium can be found by solving the following equations.

$$\begin{aligned} &\sum_{i=1}^{n} x_i = 1, and \sum_{j=1}^{m} y_j = 1 \\ &\sum_{i=1}^{n} x_i b_{ik_1} = \sum_{i=1}^{n} x_i b_{ik_2}, \forall k_1, k_2 \in S_1 \ and \ k_1 \neq k_2 \qquad (1) \\ &\sum_{j=1}^{m} y_j a_{k_1 j} = \sum_{j=1}^{m} y_i a_{k_2 j}, \forall k_1, k_2 \in S_2 \ and \ k_1 \neq k_2 \end{aligned}$$

where x_i is the frequency with which P_1 uses its ith strategy, and y_j is the frequency with which P_2 uses its jth strategy. When P_1 plays its ith strategy, and P_2 plays its jth strategy, the payoff to P_1 is a_{ij}, and the payoff to P_2 is b_{ij}. The support is denoted as $S_1 = \{i : x_i \neq 0, 1 \leq i \leq n\}$ and $S_2 = \{j : y_j \neq 0, 1 \leq y \leq m\}$.

TABLE II

PAYOFF MATRIX. THE FIRST VALUE IN EACH CELL IS THE PAYOFF OF P_1. THE SECOND VALUE IN THE CELL IS THE PAYOFF OF P_2. A = 3500. NASH EQUILIBRIUM STRATEGY PROBABILITY DISTRIBUTION

$P_2 \setminus P_1$	500B	1000B
1000 pulses/s	(664.8 Kbps, 6.8E06)	(42.96 Kbps, 7.5E06)
250 pusels/s	(2.7 Mbps, 7.4E06)	(3.55 Mbps, 6.6E6)
	prob. of action1	prob. of action2
802.11 nodes	0.600895	0.399105
jammer	0.576049	0.423951
	Throughput = 1.53 Mbps	

Experimental Results In the following, we show the gain of SPREAD through a 2×2 Packet-Size game. The matrix values are obtained from simulation. The two actions of the communication nodes are 500 bytes packet size and 1000 bytes packet size. The two actions of the jammer are jamming rates at 1000 pulses/s and 250 pulses/s. The payoff matrix is shown in Table II. The Nash equilibrium in this 2×2 game found by solving Equation 1 is also listed in Table II. The Nash equilibrium solution of the game indicates that SPREAD achieves a throughput of 1.53 Mbps. Compared with that of a non-SPREAD network, the throughput of SPREAD is 2.3 times as large as the throughput when the communication nodes use 500 bytes packet size strategy, and is 34 times higher than the throughput when the communication nodes use 1000 bytes packet size strategy.

V. FUTURE WORK

We plan to fully explore the Nash Equilibrium for the combined Packet-Size/Coding-Rate/Power-Level game. We will extend the analysis to the full spectrum of MAC models and jammer types. In the long term, we plan to model a larger class of cross-layer attacks and derive a set of complementing protocols that provide network resiliency against smart attacks.

REFERENCES

[1] DARPA, http://www.darpa.mil/ato/programs/WolfPack/index.htm.

[2] X. Geng, Y. Huang, and A. B. Whinson, "Defending wireless infrastructure against the challenge of DDoS attacks," *Mobile Networks and Applications*, 2002.

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 2001.

[4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Security Symposium*, 2003.

[5] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. MILCOM*, 2006.

[6] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, October 2002.

[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless lans," *Wiley Journal on Wireless Communications and Mobile Computing*, 2004.

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *INFOCOM*, 2003.

[9] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. MOBICOM*, 2002.

[10] C. Partridge, D. Cousins, A. W. Jackson, R. Krishnan, T. Saxena, and W. T. Strayer, "Using signal processing to analyze wireless data traffic," in *Proc. MOBICOM*, 2002.

[11] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.

[12] R. Jain and P. Varaiya, "Combinatorial exchange mechanisms for efficient bandwidth allocation," *Communications in Information and Systems*, vol. 3, 2004.

[13] A. B. MacKenzie and S. B. Wicker, "Stability of multipacket slotted aloha with selfish user users and perfect information," in *Proc. INFOCOM*, 2003.

[14] W. Qian, G. Noubir, X. Liu, and P. Ramachandra, "A framework for simultaneous evaluation of multiple vehicular ad hoc network protocols," in *Proc. V2VCOM*, 2005.

[15] IEEE, "Medium access control (mac) and physical specifications," *IEEE P802.11/D10*, 1999.

[16] Scalable Network Technologies, http://www.scalable-networks.com.

[17] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

[18] J. Nash, "Equlibrium points in n-person games," in *Proc. National Academy of Sciences*, 1950.

[19] X. Chen and X. Deng, "Settling the complexity of 2-player nash-equilibrium," in *Proc. ECCC*, 2005.

[20] A. M. Richard J. Lipton, Evangelos Markakis, "Playing large games using simple strategies," in *Proc. ACM-EC*, 2003.

[21] P. Lettieri and M. B. Srivastava, "Adaptive frame length control for improving wireless link throughput, range, and energy efficiency," in *Proc. INFOCOM*, 1998.