International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 11, October 2016

ISSN: 2394-4404

An Approach Of P2P Network For Preclusion Of Selective Jamming Attacks Using Packet Concealing Methods

Saniya Taskeen

Inchara.K

Rumana Sadiya

Students, Dept of ECE, Ghousia College of Engineering,
Ramanagaram, Karnataka

Mohammed Elahi

Asst. Professor, Dept. of ECE,
Ghousia College of Engineering, Ramanagaram, Karnataka

Abstract: Wireless sensor networks (WSNs) are used in many applications which often include the transferring data with security and data no data loss. Interfering attackers in WSN to block or grab sensitive information to be done with wireless transmissions can be used as a Launch pad for rising Denial-of-Service attacks on wireless networks. Typically, blocking has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort blocking attacks that are difficult to detect and counter. In this paper we present data concealing technique to protect data in jammer nodes and also detect jammer nodes using a selective attack on TCP and one on routing with symmetric encryption algorithm and ATR (Augmented Tree Based Routing) respectively. We also show throughput in a network, with this we show packet loss control, efficiency, coding rate, time etc, also we analyze security methods wireless sensor network. We have conducted simulation experiments. The results show that our previously proposed method is effective in both cases in which the network size is small or large. "The concept of transmission can be applied for wireless multimedia and even for peer to peer communication".

Index Terms: Selective Jamming, Denial-of-service, Wireless Networks, Packet Classification.

I. INTRODUCTION

Wireless networks are likely to be many security threats due to the open nature of the wireless medium. Anyone with a transceiver can secretly listen to a conversation on ongoing transmissions, inject fake messages, or jam the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions. In the simplest form of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's frequencies being used, and in nearness to the targeted receivers. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to spend a large enough amount of energy to squeeze frequency bands of interest. Second, the continuous presence of high interference levels, make this type of squeeze easy to detect. Third, Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmission. In this paper, we consider a highly developed and complex adversary model in which the adversary is aware of the implementation details of the network protocols. By exploiting this knowledge, the adversary launches selective jamming attacks in which it targets particular packets of "high" importance. For example, jamming of TCP acknowledgments (ACKs) can severely degrade the throughput of a TCP connection due to the congestion control mechanism of the TCP protocol. Compared to continuous jamming, the adversary is active for a short period of time, thus expending orders of magnitude less energy. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet (by decoding the frame control field of a MAC-layer frame). We are interested in developing resource efficient methods for preclusion real-time packet classification and hence, mitigating selective jamming.

OUR CONTRIBUTIONS: We carry out the feasibility of real-time packet classification for launching selective jamming attacks. We consider a highly developed and complex adversary who exploits his knowledge on network protocols along with secrets extracted from compromised nodes to maximize the impact of his attack. To mitigate selective jamming, we combine one on routing with symmetric encryption algorithm and ATR (Augmented Tree Based Routing), with physical-layer parameters. Data transmission can be shown by the routing algorithms; in most cases we can use more efficient routing algorithms for data transmission. The concept of transmission can be applied for wireless multimedia and even for peer to peer communication. This gives very efficient and most time consuming communication results. Ultimatimately prevents from jamming attacks in any other networks.

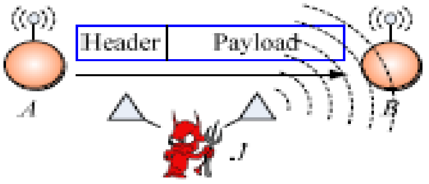


Figure 1: (a) Realization of selective jamming attacks

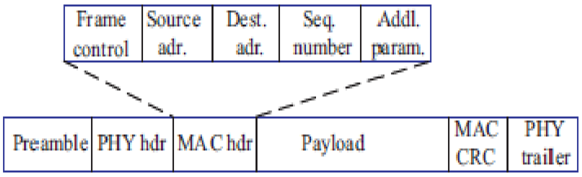


Figure 2: (b) A generic frame format for a wireless network

II. PROBLEM STATEMENT AND ASSUMPTION

A. PROBLEM STATEMENT

Consider the scenario depicted in Fig. 1(a). Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preclusion the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics.

B. SYSTEM AND ADVERSARY MODEL

NETWORK MODULE: We address the problem of preclusion the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pairwise keys.

COMMUNICATION MODEL: Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries _ _ q data bits, where α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is _ _ qR bps. Spread spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmissions from jamming. SS provides immunity to interference to some extent (typically 20 to 30 dB gain), but a powerful jammer is still capable of jamming data packets of his choosing. Transmitted packets have the generic format depicted in Fig. 1(b). The preamble is used for synchronizing the sampling process at the receiver. The PHY layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination addresses, sequence numbers plus some additional fields. The MAC header is followed by the frame body that typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.

ADVERSARY MODEL: We assume the adversary is in control of the communication medium and can block messages at any part of the network of his choosing. The adversary can carry out in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of multi-radio transceivers. In addition, the adversary is task with directional antennas that enable the receiving signal from one node and jamming of the same signal at another. For analysis purposes, we assume that the adversary creating jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality, it has been demonstrated that selective jamming can be achieved with far less resources. A jammer carry out with a single half-duplex transceiver is enough to classify and jam transmitted packets. However, our model captures a more powerful adversary that can be successful even at high transmission speeds. The adversary is assumed the mathematical calculation and storage bounded, although he can be far higher in status to normal nodes. In particular, he can be carrying out with special purpose hardware for performing cryptanalysis or any other required calculation. Solving well-known hard cryptographic problems is assumed to be time-consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be covering all aspects search on the key space. The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model has sensible and practical idea for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may carry out unattended, thus being influenced to physical compromise.

III. REAL TIME PACKET CLASSIFICATIONS

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded, to recover the original packet m.

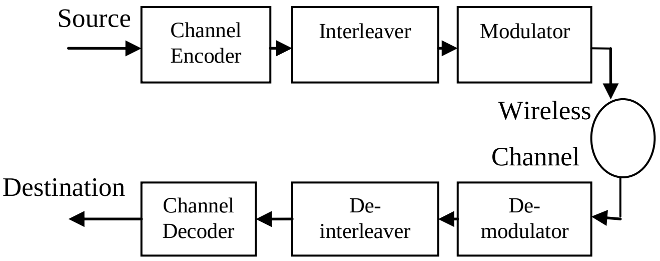


Figure 2: Generic communication system

Moreover, even if the encryption key of a concealing scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

PACKET FORWARDING PROCESS

The ATR multi-path routing exhibits temporal diversity, i.e. the Path Discovery Process performs a pre-emptive route discovery before the occurrence of route errors. Moreover, ATR could be easily extended to split a data transfer on multiple paths in the spatial domain, to reduce congestion effects and end-to-end delay. Let us describe the proposed Packet Forwarding Process. If node ‘M’ with network address [001] must forward a data packet to a node with network address [010], it first looks the entries related to the sibling the destination network address belongs to, i.e. the level-1 sibling [01X]. In this case there are two entries in the routing table, so node ‘M’ will pick up the one exhibiting the least hop count metric, i.e. the node [010]. Otherwise, if there are no entries for the level-1 sibling, node ‘M’ will expand its search to higher sibling, i.e. level-2 sibling [1XX]. Moreover, we take advantage of multi-path defining a cross layer solution to handle with link failures. If a node detects a link failure after the forwarding of a data packet, namely if it does not receive the acknowledgement, the previously used next hop is invalidated. Then the data packet will be re-forwarded using a different path already discovered by the Path Discovery Process. Evidently this leads to higher delays in packet delivery, however it is often more convenient to wait a little more instead of wasting the resources used up to here in packet forwarding. The use of this link-breakage detection technique is another difference of the proposed approach.

IV. SELECTIVE JAMMING MODULE

We illustrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first ciphertext block.

V. IMPLEMENTATION

The implementation contains software such as JDK 1.6 running in Windows XP operating system. The system uses Java technology such as RMI (Remote Method Invocation). Java’s SWING API is used to build user interface. The RMI technology lets nodes to communicate remotely. The simulation part contains three kinds of nodes namely centralized server, server and client. The purpose of source is to send the data to the destination. There sender consists of the Channel Encoder, Interleaver and the Modulator. For simulation of communication in WSN, the server node will be able to send messages to client nodes based on the port number and the communication is routed through one of the centralized servers. Here user is able to select

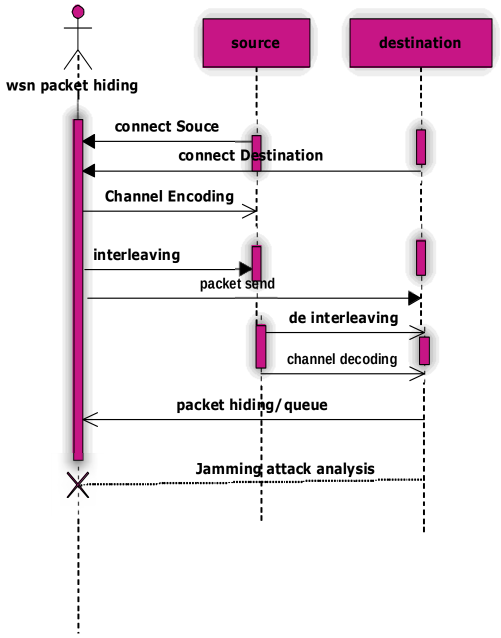
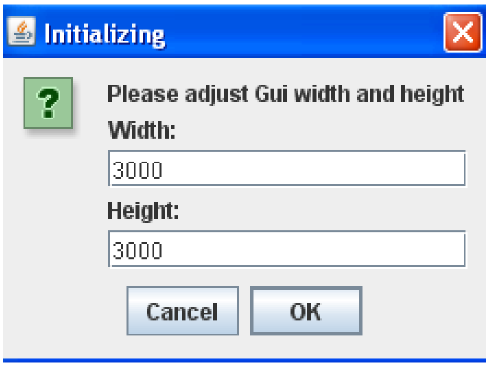


Figure 3: Sequence Diagram

File by clicking browse button. The Send button is to be initiated by user in sequence to send messages to client based on port number. The message selected is broken into packets with length 48 bytes. It selects the required data and sends it to a particular client. The data is sent in the form of packets with length 48 bytes. The server has to use specific IP address and port number based on the centralized server through which it send the messages to client.

Channel encoding deals with error control during the transmission through the communication channel. It transforms the information sequence to the encoded sequence. The result we get after modulation is "Code Word". The channel encoding will be carried out in this way. After the encoding is completed it display message. Interleaving is a method to arrange data in a non-contiguous direction to increase performance. In error-correction coding, particularly within data transmission, disk storage, and memory. After interleaving the data is converted into packets. Then the packets are used for the transmission. Identify the destination and data is converted into the packets and send to selected destination. If the data is sent successfully there will be a message in the "status information"

- ✓ *Packet Concealing Queue* Packet concealing Queue is responsible for sending the packets in a queue format i.e., first come first served the packets which arrives first will be sent first in a sequential order. The packet concealing acts as a server which is used for identifying the destination. It also checks size of the data when we are transmitting. Each packet will be storing its corresponding information in the binary format. The packet concealing queue is responsible for sending data to the destination. When the packet concealing queue sends the data received from source to the destination. The destination is ready to take the data from packet concealing queue. The destination will be receiving the path from where it can get the data from the packet concealing queue. The Destination will be consisting of Demodulator, De-interleaver and Channel decoder. Demodulation is a process used at the receiver end to recover the original signal coming from sender end in modulating form. At the receiver end, the interleaved data is arranged back into the original sequence by de-interleaver. As a result of interleaving, correlated noise introduced in the transmission channel appears to be statistically independent at the receiver end and thus allows better error correction.
- ✓ *Selected File Data at Source* Data is sent from the sender is a text file which is consist the following information.
- ✓ *Received Data at Destination* Status information text area is meant for presenting status messages.



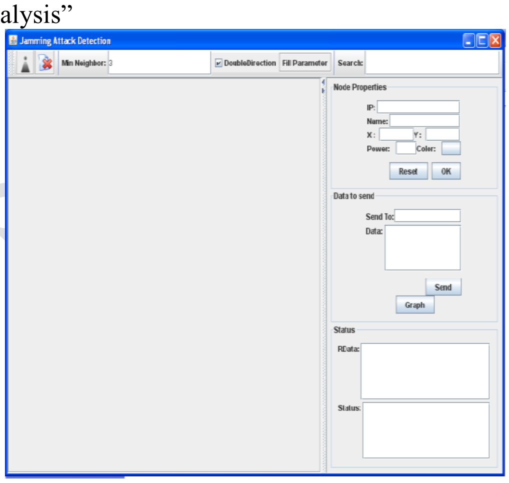
Please adjust Gui width and height

Width: 3000

Height: 3000

Figure 4: Initial Adjustment of GUI

- ✓ *The Jamming Attack Analysis* Experiments are made with two clients, two servers and a packet concealing Queue. The communication flow starts when source decides to send messages to client. It chooses a file and broken it into many packets of size 48 bytes each and sends through randomly selected centralized server. The server monitors communication and detects any jamming attacks. The jamming Attacks can be viewed by "Jamming Attack Analysis"

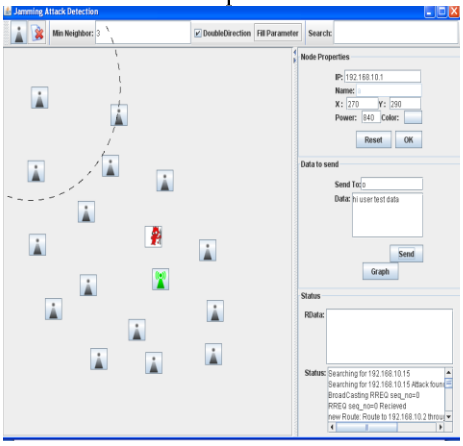


Min Neighbor: 3

☑ DoubleDirection

Figure 5: Jamming Attack Analysis

The above fig shows the jamming attack detection. There will be many numbers of nodes which we need to be added. Each node specifies a range to transmit the data. When data is sent from source to destination using the packet concealing queue It can analyze the attacks and also find whether the attack is made or not. It considers packet loss as well. It is assumed that due to attack in sending packets may occur and in turn it results in data loss or packet loss.



Min Neighbor: 3

IP: 192.168.10.1

Name: a

X: 270 Y: 290

Power: 840

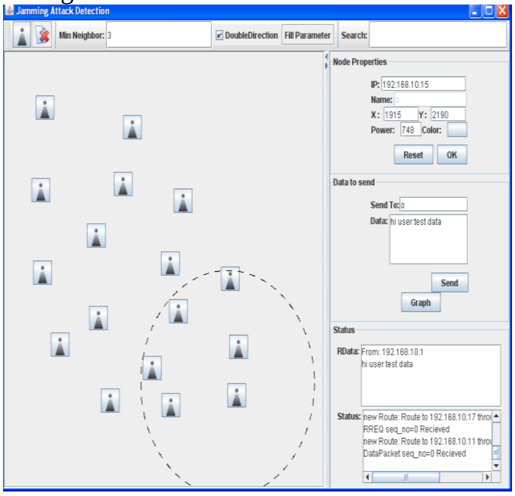
Send To: o

Data: hi user test data

Status:
Searching for 192.168.10.15
Searching for 192.168.10.15 Attack foun
BroadCasting RREQ seq_no=0
RREQ seq_no=0 Recieved
new Route: Route to 192.168.10.2 throu

Figure 6: Jamming Attack Detection

As seen in fig6 (Screen shots), when the jamming attack is detected then it will be indicated with the red symbol at the corresponding node.



IP: 192.168.10.15
Name: 0
X: 1915 Y: 2190
Power: 748 Color:

Send To: 0
Data: hi user test data

RData: From: 192.168.10.1
hi user test data

Status: new Route: Route to 192.168.10.17 throu
RREQ seq_no=0 Recieved
new Route: Route to 192.168.10.11 throu
DataPacket seq_no=0 Recieved

Figure 7: Jamming Attack Output

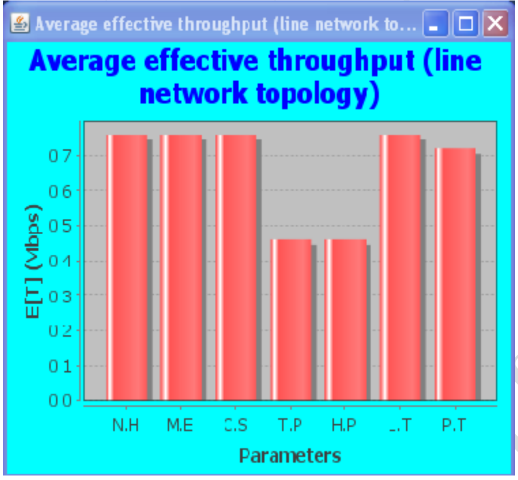


Figure 8: Average effective throughput of line network topology

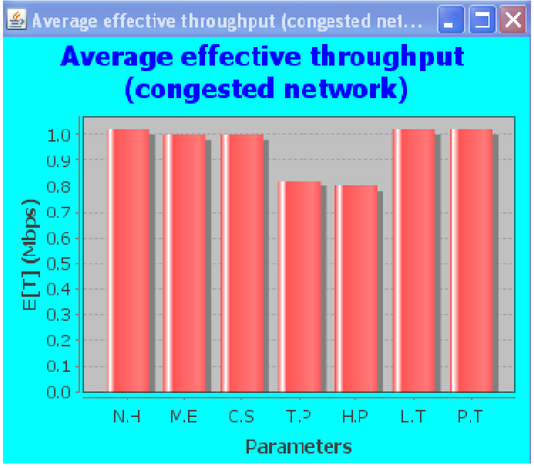


Figure 9: Average effective throughput of Congested network

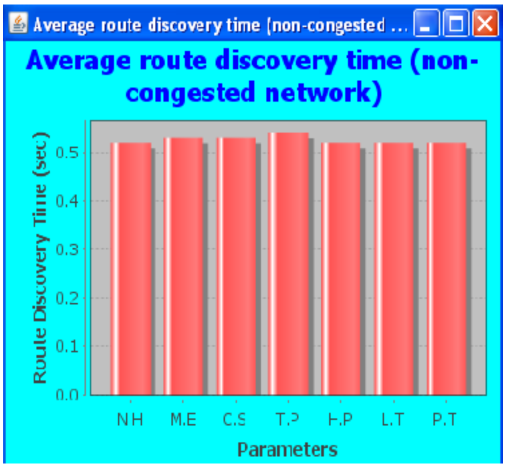


Figure 10: Average effective throughput of non- Congested network

VI. CONCLUSION

The paper proposes a hierarchical approach to protect data in jammer nodes and also detect jammer nodes using a selective attack on TCP in order to solve data security problem symmetric encryption algorithm has been used and against node failure/mobility and link congestion/instability problem ATR (Augmented Tree Based Routing) protocol is used. Simulation results and performance comparisons with existing protocols substantiate the effectiveness of the ATR.

REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[5] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[6] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

[7] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

[9] IEEE.IEEE802.11standard.http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[10] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.

[11] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[13] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.

[14] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536– 2540, 2007.

[15] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.

[16] R. C. Merkle. Secure communications over insecure channels. Com- munications of the ACM, 21(4):294–299, 1978.

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