Avoiding Selective Jam Attack by Packet Hiding Method in Wireless Sensor Network

Dilip Kumar D.P [1], H. Venugopal[2]

Student of M. Tech, Computer Science and Engineering Sri Siddhartha Institute of Technology, Tumkur, India
Department CS&E, Sri Siddhartha institute of technology, Tumkur, India

Abstract: ***the open nature of the wireless medium leaves it vulnerable to drive or wedge packets forcibly into a tight position referred as squeeze. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks typically; squeeze has been addressed under an external threat model. However, person with depth knowledge of internet protocol specifications and network secrets can launch low-effort squeeze attacks that are difficult to detect and counter. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective squeeze in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. In this work, we address the problem of selective squeeze attacks in wireless networks. We show that selective squeeze attacks can be launched by performing real-time packet classification at the physical layer. To reduce these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.***

Keywords: Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

1. Introduction

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions [9], [11], [19], and [20]. In the simplest form of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers [15]. For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise [15]. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of high interference levels makes this type of jamming easy to detect [11], [19], and [20]. Third, these attacks are easy to mitigate either by spread spectrum communications [15], spatial retreats [20], or localization and removal of the jamming nodes. In this paper, we consider a sophisticated 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 specific 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 [3]. 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, for example, by decoding the frame control field of a MAC-layer frame. We are interested in developing resource efficient methods for preventing real-time packet classification and hence, mitigating selective jamming. Our contributions are summarized below.

A. Our Contributions investigates the feasibility of real-time packet classification for launching selective jamming attacks. We consider a sophisticated 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 cryptographic mechanisms such as commitment schemes [6], cryptographic puzzles [7], and all in- one transformation [13], with physical-layer parameters. We further study the impact of various selective jamming strategies on the performance of the TCP protocol. The remainder of the paper is organized as follows. Section II represents related work. In Section III, we describe the problem addressed, and state the system and adversarial model assumptions. In Section IV, we illustrate the feasibility of selective jamming attacks. In Section V, we develop methods for preventing selective jamming. Section VI, illustrates the impact of selective jamming on the performance of TCP. In Section VII, we conclude, illustrate the feasibility of selective jamming attacks. In Section V, we develop methods for preventing selective jamming. Section VI, illustrates the impact of selective jamming on the performance of TCP. In Section VII, we conclude.

2. Related Work

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [15]. Recently, several alternative jamming strategies have been demonstrated [11], [12], [19], and [20]. Xu et. al. Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates

between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected. Intelligent attacks which target the transmission of specific packets were presented in [8], [18].

Figure 1 (a): Realization of a selective jamming attack

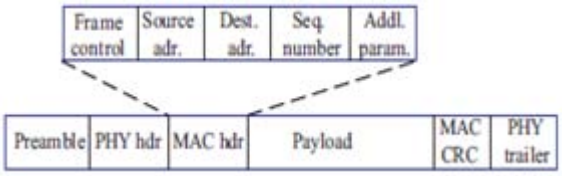

Figure 1 (b): A generic frame format for a wireless network

Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer. Law et. al. considered(a) (b) selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops. However, in both [8], [18], real-time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved via inference from the control messages already transmitted. Channel-selective jamming attacks were considered in [4], [17]. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, control information was replicated in multiple channels. The "locations" of the channels where control traffic was broadcasted at any given time, was cryptographically protected. In [9], we proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers. Finally, P¨opper et. al. proposed a frequency hopping anti-jamming technique that does not require the sharing of a secret hopping sequence, between the communicating parties [12].

3. Proposed Work

Here the contribution towards jamming attacks is reduced by using the two algorithms
1. Symmetric encryption algorithm
2. Brute force attacks against block encryption algorithms

The proposed algorithm keeps these two in mind as they are essential in reducing the jamming attacks by using the packet hiding mechanism. First we have given a security for user to enter their details in order to send the data. At that time Automatic key is generated for the particular user. Finally data is successfully inserted into database. At last we can view the user list how many people are send their files to the destination. Using that key user able to login and send the file to the destination.

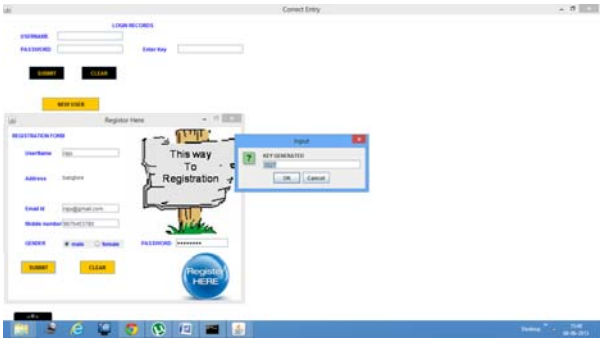

Figure 2: Login Form

4. Problem Statement and Assumptions

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 preventing 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, as described in [1], [4], [11], [33].

B. System and Adversary Model 1.

Network model 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 pair wise keys or asymmetric cryptography.

5. 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.

6. Adversary Model

We assume the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing (similar to the Dolev- Yao model). The adversary can operate 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 equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. For analysis purposes, we assume that the adversary can pro-actively 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 [32], [34]. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent adversary that can be effective even at high transmission speeds. The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. 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 an exhaustive 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 is realistic for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may operate unattended, thus being susceptible to physical compromise.

7. Implementation

The implementation environment has 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 has three kinds of nodes namely centralized server, server and client. The purpose of source is to send the data to the destination. There sender will be consisting of the Channel Encoder, Interleaver and the Modulator. For simulation of communication in WSN, the server node is 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 a file by clicking browse button. The Send button is to be initiated by user in order to send messages to client based on port number. The message or file 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 is to send the messages to client.

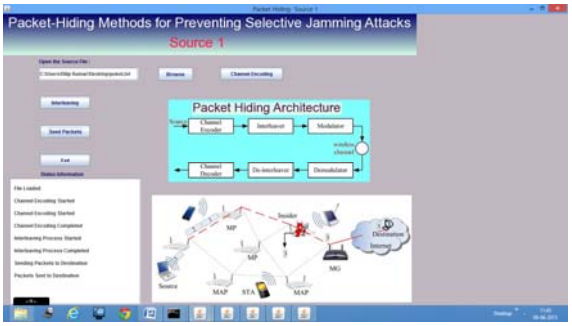

Figure 3: Packet hiding methods for preventing selective jamming attacks

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 the modulation is "Code Word". For acknowledgment of loading File the channel encoding will be done. After the encoding is completed there will be a message displayed.

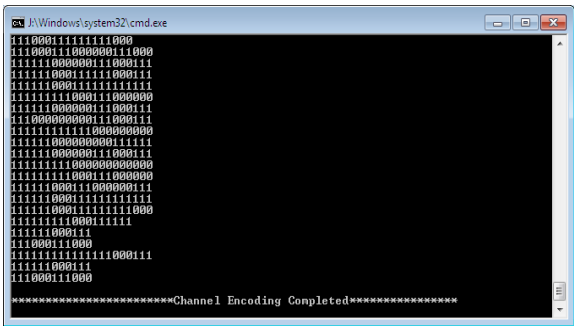

Figure 4: Channel encoding of the data

Interleaving is a way to arrange data in a non-contiguous way to increase performance. In error-correction coding, we particularly deal within data transmission, disk storage and memory. After the interleaving the data is converted into packets. Then the packets are used for the transmission

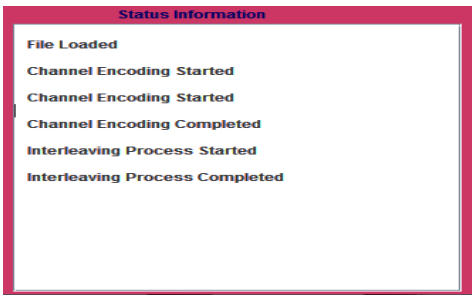

Figure 5: Status corresponding to particular action Identify the destination and data is converted into the packets and send to selected destination. If the data is sent properly there will be a message in the "status information"

Packet Transmission to the Packet hiding queue

A. Packet Hiding Queue

Packet hiding Queue is responsible for sending the packets in a queue format i.e., first come first served the packets which come first will be sent first in a sequential order. The

packet hiding acts as a server which is used for identifying the destination. It also checks the size of the data when we are transmitting. Each packet will be storing its corresponding information in the binary format. The packet hiding queue is responsible for sending the data to the destination.

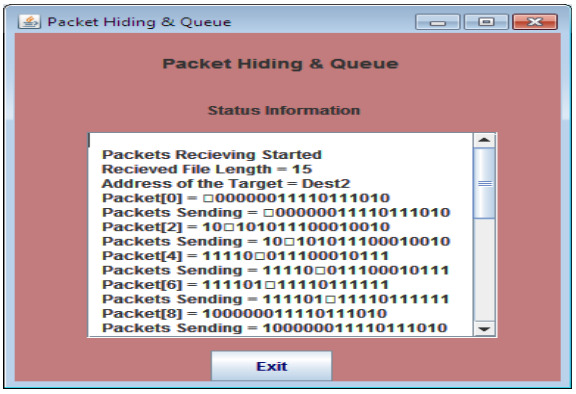

Figure 6: Packet Hiding Queue

When the packet hiding queue sends the data received from the source to the destination. The destination will be ready to take the data from the packet hiding queue.

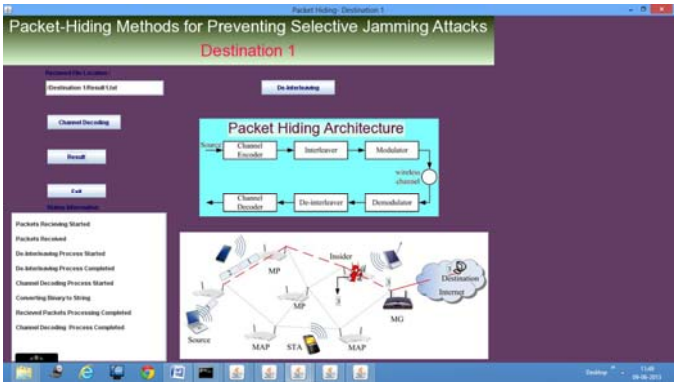

Figure 7: Packets Received at Destination

The destination will be receiving the path from where it can get the data from the packet hiding queue. The Destination will be consisting of the Demodulator, De-interleaver and Channel Decoder. Demodulation is a process used in the receivers to recover the original signal coming from the sender end in modulating form. At the receiver end, the interleaved data is arranged back into the original sequence by the **de-interleaver**. As a result of interleaving, correlated noise introduced in the transmission channel appears to be statistically independent at the receiver and thus allows better error correction. Status After demodulation, deinterleaving and channel decoding

B. Selected File data at the Source

The data sent from the sender is a text file which consist the following information. Choose file with the data at Source.

C. Received Data at Destination

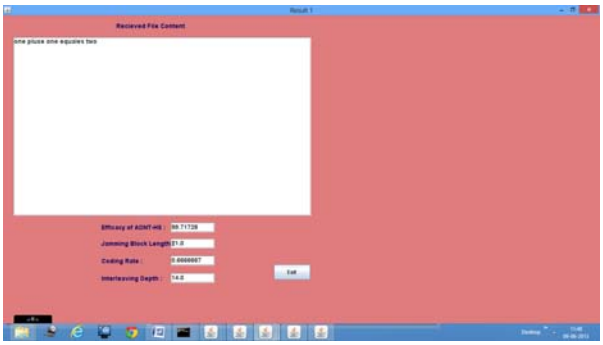

Figure 8: Received data at the destination

The status information text area is meant for presenting status messages.

D. The Jamming Attack Analysis Experiments

These are made with two clients, two servers and a packet hiding Queue. The communication flow starts when source decides to send messages to client. It chooses a file and breaks it into many packets of size 48 bytes each and sends them through randomly selected centralized server. The server monitors communication and detects any jamming attacks. The jamming Attacks can be viewed by “Jamming Attack Analysis”. It shows the jamming attack detection. There will be many numbers of nodes which we need to be added. Each node will be having a range to transmit the data, when data is sent from source to destination by using the packet hiding 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.

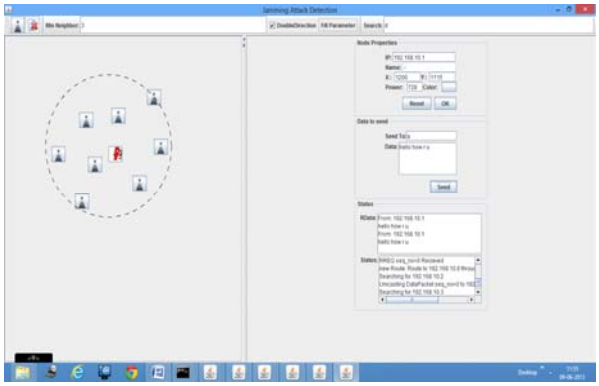

Figure 9: Jamming Attack Detection

As seen in fig, the when the jamming attack is detected then it will be indicated with the red symbol at the corresponding node

8. Conclusion

We addressed the problem of selective jamming in wireless networks. We illustrated the effectiveness of selective jamming attacks by implementing such attacks against the TCP protocol. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of selective jamming attacks by

performing real time packet classification. To mitigate selective jamming, we proposed several methods that combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all- or-nothing transformations with physical layer attributes.

References

[1] Onetime modeler 14.5. http://www.opnet.com/solutions/network rd/ modeler.html.

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

[3] Al Hanbali, E. Altman, and P. Nain. A survey of tcp over ad hoc networks. IEEE Communications Surveys & Tutorials, 7(3):22–36, 2005.

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

[5] D. Comer. Internetworking with TCP/IP: principles, protocols, and architecture. Prentice Hall, 2006.

[6] Damgard. Commitment schemes and zero-knowledge protocols. Lecture notes in computer science, 1561:63–86,

[7] Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of the Network and Distributed System Security Symposium, pages 151–165, 1999.

[8] 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. ACM Transactions on Sensor Networks, 5(1):1–38, 2009.

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

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

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

[12] Po¨pper, M. Strasser, and S. C˘ apkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[13] R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.

[14] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timed-release crypto. 1996.

[15] M. Simon, J. Omura, R. Scholtz, and B. Levitt. Spread spectrum communications handbook. McGraw-Hill Companies, 1994.

[16] Stinson. Cryptography: theory and practice. CRC press, 2006.

[17] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of the PIMRC, 2007.

[18] Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In Proceedings of the IEEE MILCOM, 2006.

[19] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 46–57, 2005.

[20] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 3rd ACM workshop on Wireless security, pages 80–89, 2004

Author Profile

Dilip Kumar D.P has received a graduation from Visvesvaraya Technological University Belgaum during 2010-11; currently I am perusing my post graduation (M. Tech) in the department of computer science and engineering 2012-13, from Sri Siddhartha academy of higher education Tumkur.