ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

Security of Vulnerable Wireless Network Systems and its attacks on Jamming

Y. Deepika[1], Dr. A. Govardhan[2], Dr. N. Chandra Sekhar Reddy[3]

Student, M.Tech SE Department, Institute of Aeronautical Engineering, Hyderabad, Telangana, India[1]

Professor, Department of CSE & Director SIT, JNTUH, Kukatpally, Hyderabad,Telangana,India[2]

Professor, CSE Department, Institute of Aeronautical Engineering, Hyderabad, Telagana, India[3]

Abstract: This paper deals with the latest technology called the Security of Vulnerable Wireless Network Systems & Its Attacks of Jamming. In this we are going to describe the security problems of wireless networks and the Jamming attacks of wireless networks and the jamming attacks which are occurred in network. Network is a group or System of interconnected people or things which are used for passing the information. We have two types of networks. They are Wired network & wireless network. Now we are working on Wireless networking. The Nature of Wireless medium has a chance to get easily attacked by intentional interference attacks which is called as Jamming. Then this intentional interference with wireless transmission can be used as launch pad for mounting Denial-Of-Service attacks on wireless networks. In this we are having some important methods to develop the security. We analyze the security of our methods and evaluate their computational & communication overhead.

INTRODUCTION

Wireless networks completely depend on signals and frequency modulation. Wireless networks depend on the wireless medium (uninterrupted wireless network) to connect all the nodes which are participating. The wireless medium leaves intentional interference called jamming. Normally jamming has been addressed under an external thread model. Anyone with any transceiver can eavesdrop on wireless transmission, jam legitimate ones inject spurious messages.

Jamming attacks are much harder to find out and very much harder to solve it. It is shown to actualize the severe, Denial of service (DOS) attacks against the wireless networks.

Jamming attacks have been considered in an external threat model. Though, adopting an "always-on" strategy has several disadvantages. Initial, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Next, the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Conservative anti-jamming techniques rely extensively on spread spectrum (SS) communications. SS techniques provide a bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. In this we have some methods and schemes for preventing jamming attacks.

2. RELATED WORK

In this section, we describe how the adversary can classify packets in real time,previous to the packet transmission is completed. Formerly a packet is classified; the adversary may wish to jam it depending on his strategy. Believe the generic communication system depicted in Fig. 1. At the PHY layer, a packet m is interleaved, encoded and modulated before it is transmitted over the wireless channel. By the receiver, the signal is deinterleaved, demodulated and decoded, to recover the original packet m.

The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 1. The channel encoding block expands the original bit sequence m, adding basic redundancy for protecting m against channel errors. For illustration, α/β- source

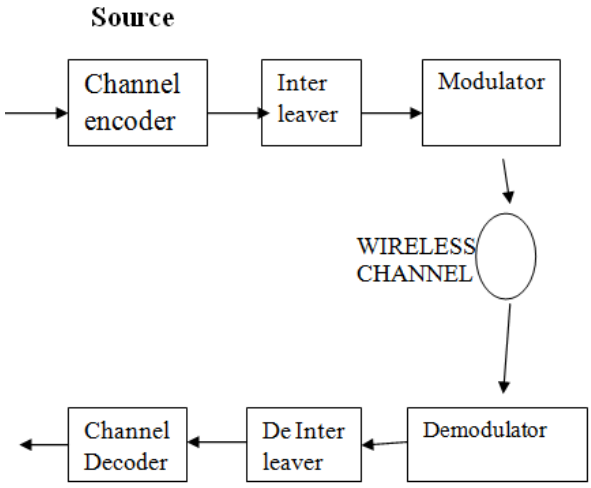


Fig. 1. A generic communication system diagram.

Block code may protect m from up to e Errors per block. on the other hand, an α/β-rate convolution encoder with a constraint length of Lmax, also a free distance of e bits provides similar protection. For our purposes, we suppose

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

that the rate of the encoder is α/β. By the next block, interleaving is applied to protect m from burst errors. For simplicity, we believe a block interleaver that is defined by a matrix Ad×β1.
The de-interleaver is simply the
transpose of A. Lastly; the digital modulator maps the received bit stream to symbols of length q, also modulates them into suitable waveforms for transmission over the wireless channel. Typical modulation techniques consist of OFDM, BPSK, 16(64)-QAM, and CCK. In order to recover any bit of m, the receiver should collect d · β bits for deinterleaving. The d · β de-interleaved bits be passed through the decoder. Ignoring any propagation and decoding delay, the delay until decoding the first block of data is ⌈ dβ/q ⌉ symbol durations. A standard, in use at the lowest rate of 6 Mbps, data is passed via a 1/2-rate encoder by mapped to an OFDM symbol of q = 48 bits.

In this case, decoding of one symbol provides 24 bits of data. At the maximum data rate of 54 Mbps, 216 bits of data are improved per symbol. From our study, it is evident that intercepting the first few symbols of a packet is sufficient for obtaining relevant header information. For model, consider the transmission of a TCP-SYN packet used for establishing a TCP connection at the transport layer. A PHY layer with a transmission rate of 6 Mbps. By the PHY layer, a 40- bit header and a 6-bit tail are appended to the MAC packet carrying the TCP-SYN packet. By the next stage, the 1/2-rate convolution encoder maps the packet to a sequence of 1,180 bits. In rotate, the output of the encoder is split into 25 blocks of 48 bits each and interleaved on a per-symbol basis.

Lastly, each of the blocks is modulated as an OFDM symbol for transmission. The information controlled in each of the 25 OFDM symbols is as follows:
Symbols 1-2 contain the PHY-layer header and the first byte of the MAC header. The PHY header reveals the length of the packet, the transmission rate, and the synchronization information. The initial byte of the MAC header reveals the protocol version and the type and subtype of the MAC frame (e.g.,DATA, ACK).

Symbols 3-10 contain the source, destination MAC addresses, and the length of the IP packet header.
Symbols 11-17 contain the source and destination IP addresses, size of the TCP datagram carried by the IP packet, and other IP layer information. The initial two bytes of the TCP datagram reveal the source port.

Symbols 18-23 contain TCP destination port, sequence number, acknowledgment number, TCP flags, window size, and the header checksum. Symbols 24-25 contain the MAC CRC codes. Our example illustrates that a packet can be classified at different layers and in
various ways. MAC layer classifications are achieved by receiving the first 10 symbols.
And IP layer classification is achieved by receiving symbols 10 and 11, also TCP layer classification is achieved by symbols 12-19.

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. Though, for broadcast communications, then this static decryption key must be known to all intended receivers and ,it is susceptible to compromise. An adversary in control of the decryption key can start decrypting as early as the reception of the first ciphertext block. For model, consider the cipher-block chaining (CBC) mode of encryption. To encrypt a message m with a key k and an initialization vector IV, message m is divide into x blocks m1, m2, . . .mx, and each ciphertext block ci generated as:
c1 = IV, ci+1 = Ek(ci ⊕mi), i = 1, 2, . . . , x,
(1)
where Ek(m) denotes the encryption of m with key k. The plaintext mi is recovered by:

mi = ci ⊕Dk(ci+1), i = 1, 2, . . . , x. (2)

Note from (2) that reception of ci+1 is
sufficient to recover mi if k is known (c1 = IV is also known). Therefore, realtime packet classification is still possible. One result to the key compromise problem would be to update the static key whenever it is compromised.
However, such a solution is not useful if the compromised node obtains the latest key. This can only be avoided if there is a mechanism by which the set of compromised nodes can be recognized. Such a task is nontrivial when the leaked key is shared by multiple nodes. Any node that possesses the mutual key is a candidate malicious node. Moreover, even if the encryption key of a hiding scheme were to remain underground, the static portions of a transmitted packet could potentially lead to
packet classification. This is used for
Computationally-efficient encryption methods such as block encryption, then the encryption of a prefix plaintext with the same key yield a static cipher text prefix. So, 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.

3. IMPACT OF SELECTIVE JAMMING

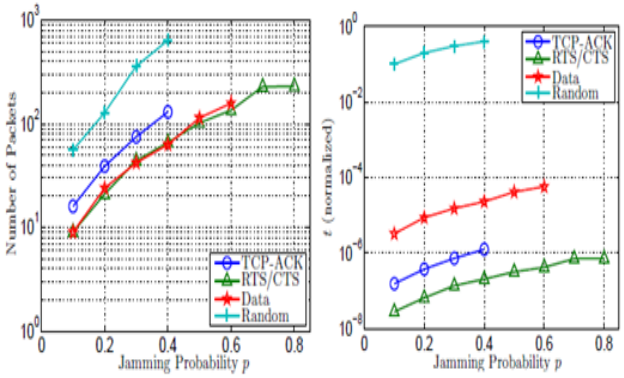
In this section, we illustrate the impact of selective jamming attacks on the network performance. To implement selective jamming attacks in two multi-hop wireless network scenarios. In the initial scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the next scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

Selective Jamming at the Transport Layer

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

In the first set of experiments, we group a file transfer of a 3 MB file between two users A and B connected via a multi-hop route. The TCP protocol was used to dependably transport the requested file. At the MAC layer, the RTS/CTS device was enabled. The transmission charge was set to 11 Mbps at each link. The jammer was located within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were measured: (a) choosy jamming of cumulative TCP-ACKs, (b) choosy jamming of RTS/CTS messages, (c) choosy jamming of data packets, and (d) random jamming of any packet. In each of the strategies, a portion p of the targeted packets is jammed.



In Fig. 2(a), we show the average delay E[D] for completing the file move, as a function of the jamming probability p (averaged over repeated experiments). In Fig. 2(b), we show the average throughput E[T] as a function of p. It can be convenient that all jamming attacks have significant impact on E[D] which grows several orders of magnitude larger compared to the delay in the absence of a jammer. also, the effective throughput drops drastically under both random and selective jamming attacks. TCP presentation under jamming of TCP-ACKs can be interpreted by the congestion control mechanism of the TCP protocol.

When cumulative ACKs are lost (in our case jammed), then the sender has to retransmit all unacknowledged data packets, so increasing the incurred delay while
reducing the effective throughput. At the equal time, the sender interprets the loss of ACKs as congestion and throttles its packet transmission rate by reducing the size of the transmission window. This leads to a advance slowdown of the application. Note that, for values of p > 0.4, the TCP connection is aborted for the case of random and TCP-ACK jamming, due to the repeated timeouts at the sender.

Fig. 2(c) depicts the number of packets that were jammed by the adversary for each value of p. Finally, Fig. 2(d) shows the fraction of time that the jammer remained active. At this point, for selective jamming attacks, we assumed that 13% of the packet has to be corrupted in order to be dropped. In the case of random jamming, the opponent is not aware of the type of packets transmitted (by means of processing the header of these packets). So, he is assumed to jam the entire packet in order to drop it. We examine that selective jamming requires the jamming of approximately one order of magnitude less packets than random jamming.

This is since, as the packet transmission rate of the sender drops fewer packets need to be selectively targeted. additionally, in selective jamming, the portion of time the adversary remains Active is several orders of magnitude less compared to random jamming. From Fig. 2(d), we observe that targeting control packets such as RTS/CTS messages and TCP-ACKs yields the lowest jamming activity, since control packets are significantly smaller compared to data packets.

Then such low-effort jamming attacks are not only efficient in terms of energy expenditure, however also challenging in localizing and physically removing the jamming devices. distinctive methods of transmitter localization such as received signal strength and angle of arrival measurements require that the jamming device remains active for extended periods of time.

4. HIDING BASED ON CRYPTOGRAPHIC PUZZLES

In this section, we present a packet hiding scheme based on cryptographic puzzles. The main idea last such puzzles is to force the recipient of a puzzle execute a predefined set of computations before he is able to extract a secret of interest. Then the time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. Though, it has higher computation and communication overhead.

Sender S **Receiver**

Generate: k, t_p C^I, P^I

Compute
P=puzzle(k,t_p) ⟶ Compute:m^I

C=$E_k(\prod_1(m))$ $=\prod_1^{-1}(D_k(C^{1}))$
Verify: m^1 is meaningful if not : discard m^1

Fig.3. The cryptographic puzzle-based hiding scheme.

In our context, we use cryptographic
puzzles to temporary hide transmitted packet.

A packet m is encrypted with a randomly selected symmetric key k of a desirable length. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally surrounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted

version of m is completed and the puzzle is received. So, the adversary cannot classify m for the purpose of selective jamming.

5. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered the internal adversary model in which the jammer is part of the network under attack, so being aware of the protocol specifications and shared network secrets. We showed that the jammer can categories transmitted packets in real time by decoding the first few symbols of ongoing transmissions. We evaluated the impact of selective jamming attacks on network protocols such as routing and TCP. Our findings show that a selective jammer can significantly impact performance with very low efforts. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classifications. Our schemes combine cryptographic primitives such as cryptographic puzzles, commitment schemes and all-or-nothing transformations (AONTs) with physical layer characteristics. We analyzed the quantified their computational, security of our schemes and communication overhead.

REFERENCES

[1] http://networking.ncsu.edu/ThuenteMilcom06_FINAL.pdf
[2] http://www2.engr.arizona.edu/~llazos/papers/LAZOS_ICC10.pdf
[3] http://en.wikipedia.org/wiki/Wireless_signal_jammer
[4] http://www2.engr.arizona.edu/~llazos/papers/PROANO_TDSC11.pdf
[5]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.
[6] 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.
[7] 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.
[8] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.
[9] R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.