PREVENTION TECHNIQUES FOR JAMMING INTRUSIONS IN WIRELESS NETWORKS

M. Ravi Kumar Reddy¹, P. Naveen Sundarkumar²

¹M.Tech Student, Dept of CS, Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal (A.P), India.
²Assistant Professor, Dept of CS, Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal (A.P), India.

ABSTRACT

A wireless network depends on the continuous accessibility of the wireless medium to communicate participating nodes and the unlock environment of this medium leaves it susceptible to numerous security threats. The nature of wireless medium is exposed to intended intrusion attacks which are referred as jamming. With wireless transmissions this intended intrusions can be used as launch pad for increasing Denial of Service attacks on wireless network. The problem of selective jamming attacks in wireless and the packet loss over the wireless communication and the congestions are described in this paper. We demonstrate that by performing real time packet classification at the physical layer the selective jamming attacks can be launched and two case studies for selective jamming were proposed in terms of network performance degradation and adversary efforts are first is a selective attack on TCP and one on routing. Three approaches were to develop for preventing the real time packet classification by combining cryptographic primitives with physical-layer attributes in order to moderate these attacks.

Keywords: Wireless networks, Jamming attacks, Packet loss, Congestions, Intended Intrusion attacks.

1. INTRODUCTION

A wireless network depends on the unremitting accessibility of the wireless medium to correspond with the participating nodes and the release environment of this medium leaves it susceptible to numerous security threats [1,3,5]. A person can overhear on wireless transmissions, insert false messages, or jam genuine ones by having a transceiver. For an instance the attacker opens a private channel on an ordinary server and spreads malwares on victim computers and gives commands for his malicious purposes which is shown in fig 1. Eavesdropping and message injection can be prohibited using cryptographic methods while jamming attacks are much harder to counteract. An external threat model has been considered by jamming attacks, in which the jammer is not a part of the network [2,4]. Jamming strategies include the continuous or random transmission of high power interference signals in this model. The spread-spectrum (SS) communications or jamming evasion depends on anti-jamming techniques [6,8]. A complicated adversary who is aware of network secrets and the implementation details of network protocols are considered at any layer in the network.
stack and make use of his inner information for introducing selective jamming attacks in which specific messages of high importance are targeted [7,9,10]. The jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address in the concluding method.

![Fig 1: Attacker spreading malwares on victim computers](image)

**2. STRATEGIES BASED ON THE NATURE OF SELECTIVITY**

The evaluation of the probability allocation of inter-packet communication times for different packet types based on network traffic analysis the different packet types are estimated by the probability distribution of inter-packet transmission times [11,13]. Upcoming communications at a range of layers were predicted using approximate timing information. Selective jamming techniques are proposed for well-known sensor network MAC protocols. The numerous packet identifiers for encrypted packets such as packet range, particular instance information of different protocols and physical signal sensing are considered by them [12,15]. The unification of packet characteristics such as the minimum length and inter-packet timing was proposed to prevent selectivity. At different layers of the network stack the adversary was assumed to target control messages. From the transmitted packets in which the protocol hides all explicit identifiers which are proposed by Greenstein et al, and by encrypting them with keys only known to the intended receivers. Channel-selective jamming attacks have been suggested by several researchers, in which the jammer targets the broadcast control channel. In non-selective jamming the larger bandwidth following a PN sequence is spread through transmitted signal [14,16]. A large amount of energy is required to interfere with an ongoing transmission without the knowledge of this sequence. The advantages of SS neutralize the PN code by sharing commonly in case of broadcast communications. Jammers were classified into four types by Xu et al.: 1. constant jammer, 2. deceptive jammer that broadcasts untrue messages, 3. arbitrary jammer 4. Spontaneous jammer jams only when the action is sensed [17,18]. Studies were conducted on the problem of identifying the presence of jammers by computing the performance metrics.
3. IMPACT OF ATTACKS ON NETWORK FUNCTIONS

By making the use of knowledge of network protocols and cryptographic primitives extracted from compromised nodes are relatively easy to actualize such attacks [19]. For launching selective jamming attacks under an internal threat model the feasibility of real time packet classification are examined. With very low effort on behalf of the jammer the selective jamming attacks has lead to a Denial-of-Service which are indicated by our findings. Three systems that prevent classification of transmitted packets in real time to lessen such attacks were to develop [20]. With minimal impact on the network performance, the security of our schemes is analyzed and shows that they achieve strong security properties.

4. JAMMING OF THE MESSAGES USING SYSTEM ADVERSARY MODEL

Adversary can pack communication at any part of the network and was believed to be in command of the communication medium and can operate in full-duplex mode. A more effective adversary that can be effective even at high transmission speed is captured. A single half-duplex transceiver is sufficient to classify and jam transmitted packets with a jammer. Special purpose hardware is used for performing cryptanalysis or any other required computation and they are assumed to be time consuming. The selective jamming can be achieved with far less resources are demonstrated in real. The most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space by analyzing the given ciphertext. The adversary is able to physically negotiate the network devices and can retrieve the stored information. This internal adversary representation is practical for network architectures.

5. CONCLUSION

A selective jammer can significantly impact performance with very low effort is proposed in our paper. An internal adversary model in which the jammer is part of the network under attack is considered, and thus being aware of the protocol specifications and shared network secrets. Decoding the first few symbols of an ongoing transmission are classified by the jammer by the transmitted packets in real time is shown. The security and quantified computational and communication overhead of our schemes are analyzed. The three systems which transform a selective jammer to a random one by preventing real-time packet classification are developed. The cryptographic primitives, cryptographic problems, and all conversions with physical layer features are shared with the systems.

REFERENCES


