IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 13, Issue 2 (Jul. - Aug. 2013), PP 57-59
www.iosrjournals.org

Jamming Anticipation and Convolution through Immaculate Hiding Process of Packets

T. Sandeep[1], Ms.P.Subhadra[2]
[1](*Master of Technology, Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India,*
[2](*Associate Professor Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India)*

Abstract: Cached data not only replies local access, but also replies data request issued from other nodes. Wireless Mesh Networks (WMNs) have emerged as an important technology in building next generation fixed wireless broadband networks that provide low cost Internet access for fixed and mobile users. Reduce the number of hops that request/data need to travel in the network. In these attacks, the adversary selectively targets specific packets of "high" importance by exploiting his knowledge on the implementation details of network protocols at various layers of the protocol stack. We illustrate the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol. We show that such attacks can be launched by performing real-time packet classification at the physical layer. We study the idealized case of perfect knowledge by both the jammer and the network about the strategy of one another, and the case where the jammer or the networks lack this knowledge. The latter is captured by formulating and solving optimization problems, the solutions of which constitute best responses of the attacker or the network to the worst-case strategy of each other.

Keywords: *Denial-of-service, jamming, Wireless network, packet classification*

I. Introduction

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. As these networks gain popularity, providing security and trustworthiness will become an issue of critical importance. Many wireless security threats may be addressed through appropriately designed network security architectures which are essentially modifications of traditional security services, such as confidentiality, authentication, and integrity to the wireless domain. Wireless networks, however, are susceptible to threats that are not able to be adequately addressed via cryptographic methods. One serious class of such threats are attacks of radio interference. This exposes them to passive and active attacks, which are different in their nature and objectives. In the former, a malicious entity does not take any action except passively observing ongoing communication, e.g. eavesdropping so as to intervene with the privacy of network entities involved in the transaction. On the other hand, an active attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the attacker abuses a protocol with the goal to obtain performance benefit itself, the attack is referred to as misbehavior. If the attacker does not directly manipulate protocol parameters but exploits protocol semantics and aims at indirect benefit by unconditionally disrupting network operation, the attack is termed jamming or Denial-of-Service (DoS), depending on whether one looks at its cause or its consequences.

Jamming can disrupt wireless transmission and can occur either unintentionally in the form of interference, noise or collision at the receiver side or in the context of an attack. A jamming attack is particularly effective since (i) no special hardware is needed in order to be launched,
(ii) it can be implemented by simply listening to the open medium and broadcasting in the same frequency band as the network and
(iii) if launched wisely, it can lead to significant benefit with small incurred cost for the attacker

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. 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. Third, these attacks are easy to mitigate either by spread spectrum communications, spatial retreats, or localization and removal of the jamming nodes.

II. Background Work And Literature Survey

Intelligent attacks which target the transmission of specific packets were presented. Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer Channel-selective jamming attacks were considered. 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. We proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers. The jammer controls probability of jamming and transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network, namely by a monitoring node, and a notification message is transferred out of the jamming region. The fundamental tradeoff faced by the attacker is the following: a more aggressive attack in terms of higher jamming probability or larger transmission range increases the instantaneously derived payoff but exposes the attacker to the network and facilitates its detection and later on its isolation. In an effort to withstand the attack and alleviate the attacker benefit, the network adapts channel access probability. In Strong Hiding Commitment Scheme we use DES algorithm to encrypt packets where single secret key is used between sender and receiver. The major disadvantage is, the attacker can easily retrieve the packets based on brute force attacks so we need to provide more security for the packets. In Cryptographic puzzle Hiding Scheme, where each packet is attached with the puzzle and encrypted. We specify the time limit for the solution of the puzzle. If puzzle is not solved within the time limit there may be dropping of packets and also there is a delay in receiving the packets. Selective jamming attacks have been experimentally implemented using software defined radio engines. USRP2-based jamming platform called RF React was implemented by Wilhelm that enables selective and reactive jamming. We develop three schemes that prevent jamming attacks; they are Strong Hiding Commitment Scheme, Cryptographic Puzzle Hiding Scheme and All or Nothing Transformation

III. Problem Statement And Model Assumptions

Consider the scenario depicted in Figure 1(a). Nodes A and B communicate over the wireless medium and a jamming node J is within communication range of both A and B. Node A transmits a packet m to B which is eavesdropped by node J. Node J is able to classify m by receiving only its first few bytes. J then corrupts m by interfering with its reception at B. We address the problems of

(a) evaluating the ability of the adversary in classifying transmitted messages in real-time, and

(b) developing resource-efficient mechanisms for preventing real-time packet classification.

Network model–Our network consists of a collection of nodes connected via wireless links. Nodes may communicate directly, or over multiple hops. The nodes of the network can establish globally shared keys, either by manual preload, or via an online key distribution center. Communication Model–Communication can be either broadcast or unicast. Packets are transmitted at a rate of R bauds. Each symbol corresponds to q bits according to the underlying digital modulation scheme. Here the transmission bit rate is equal to qR bps. To generalize our analysis, we do not consider any spreading of the data. However, our results hold even if data is spread to a wider spectrum according to any technique such as DSSS or FHSS. Transmitted packets have the generic frame format depicted in Figure 1(b). The preamble is used for synchronizing the sampling process at the receiver. The PHY header contains information regarding the length of the frame and the transmission rate.

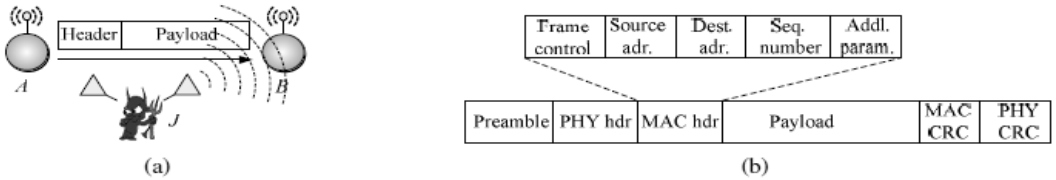

Fig. 1. (a) Realization of a selective jamming attack, (b) a generic frame format for a wireless network

The MAC header contains information relevant to the MAC layer. In particular, the MAC header determines the MAC protocol version, the type of packet (management, control, or data) and its subtype (e.g. association request/response, RTS, CTS, ACK, etc.), the source and destination addresses plus some additional fields regarding power management, security parameters, and information for future transmissions. The MAC header is followed by the frame body that contains higher layer information. Finally, the MAC frame is protected by a CRC code attached in the CRC field. 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. The adversary can

operate in full-duplex mode, thus being able to receive and transmit concurrently. This can be achieved, for example, with the use of multiple radios. 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. The adversary is assumed to be computationally bounded, although he can be significantly more powerful than the network devices. Solving well-known hard cryptographic problems is assumed to be time-consuming.

The network employs a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism consists of the following: (i) determination of a subset of nodes M that will act as network monitors, and (ii)

Employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications. In this work, we fix M and formulate optimization problems for one or more monitor nodes. We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In

Our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received. During normal network operation, and in the absence of a jammer, we consider a large enough training period in which the monitor node "learns" the percentage of collisions it experiences as the long-term average of the ratio of number of slots in which there was a collision over total number of slots of the training period. Assume now the network operates in the open after the training period and fix attention to a time window much smaller than the training period. An increased percentage of collisions over this time window compared to the learned long-term average may be an indication of an ongoing jamming attack or only a temporary increase of percentage of collisions compared to the average during normal network operation.

IV. Conclusion

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.

Therefore, to improve detection, we introduced the notion of consistency checking, where the packet delivery ratio is used to classify a radio link as having poor utility, and then a consistency check is performed to classify whether poor link quality is due to jamming. There exist several directions for future study. Interesting issues arise in multi-channel networks. In that case, the defense strategy space has an additional dimension, channel switching, while the jammer has higher energy costs when jamming more channels. Another interesting issue is to find alternatives for modeling lack of knowledge for the attacker and the network. An idea would be to average over all strategies of the opponent.

References

[1] IEEE Std 802.11i/d3.0. Available at http://www.cs.umd.edu/ mhshin/doc/802.11/802.11i-D3.0.pdf.

[2] AusCERT. AA-2004.02 - denial of service vulnerability in IEEE 802.11 wireless devices. http://www.auscert.org.

[3] P. Bahl and V. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In Proceedings of IEEE Infocom 2003, pages 775 to784, 2000.

[4] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In Proceedings of the USENIX Security Symposium, pages 15 to 28, 2003.

[5] S. Capkun and J. Hubaux. Secure positioning in sensor networks. Technical report EPFL/IC/200444, May 2004

[6] I. Damgard. Commitment schemes and zero-knowledge protocols. Lecture notes in computer science, 1561:63–86, 1999.

[7] A. 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] W. Xu, W. Trappe, Y. Zhang and T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks,Proc. ACM Mobi Hoc, 2005.

[12] W. Xu, T. Wood, W. Trappe and Y. Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service, Proc. Workshop on Wireless Security (WiSe), 2004.

[13] J. M. McCune, E. Shi, A. Perrig and M. K. Reiter, Detection of denial-of-message attacks on sensor network broadcasts ,Proc. IEEE Symposium on Security and Privacy, 2005.

[14] A. Wald, Sequential Analysis, Wiley 1947.