SELECTIVE JAMMING ATTACK PREVENTION ALGORITHM IN POCKET DELAY NETWORKS

G Kumara swamy[#1], S Anjaneyulu[*2],Santhosh Kumar seelam[#3]

[#]*Department of Computer Science , JNTUH*

[1]kumaraswamy.drm@gmail.com

[3]santhu3513@gmail.com

[*]*JNTUH,INDIA*

[2]*anjan_sb@yahoo.com*

***Abstract*— This paper discusses exclusively the role of jamming at the Trans port/Network layer. The Link/Physical layer provides a sensing and jamming service. The jamming service is defined as jamming for abased attacks. In this paper we consider encrypted victim networks in which the entire packet including headers and payload are encrypted and thus the attacker can not directly manipulate any of the victim communication. 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 rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks [12], [17], [36], [37]. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal [25], or several short jamming pulses [17].

Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals [25], [36]. However, adopting an "always-on" 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 unusually high interference levels makes this type of attacks easy to detect [17], [36], [37].

Conventional anti-jamming techniques rely extensively on Spread-spectrum (SS) communications [25], or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats [37]). SS techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

2 PROBLEM AND SOLUTION OVERVIEW

Consider the scenario depicted in Fig. 1a. 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].

3 THE ROLE OF ENCRYPTION

MAC protocols can have various levels of encryption. HTTPS, SSH, or IPSec can encrypt packet payloads at layer 3 or higher but do not encrypt MAC and Ad Hoc network information. 802.11 Wired Equivalent Privacy (WEP) and Wifi Protected Access (WPA) both are designed to protect the contents of the packet but not the control information in the MAC header [18]. Some implementations go further and also encrypt the entire

MAC header [11]. In this paper, we assume that the entire packet is encrypted and only size and packet timing information can be measured. The main difference then is that encryption may change the packet size by an unknown amount. Some encryption schemes add a fixed offset in the packet size that, as we will see, does not impose serious difficulties on the sensing. Another type of encryption is exemplified by the 802.11i WPA2 protocol. This protocol uses a block encryption so that all packet sizes are rounded up to the nearest multiple of 128 bits. This tends to reduce the fidelity of the sensing since similar Page Layout, an easy way to comply with the journal paper formatting requirements is to use this document as a template and simply type your text into it.

4 JAMMING MECHANISMS IN AD HOC NETWORKS

In network protocols, certain critical packets are necessary for operation. Jamming TCP-SYN or TCP-SYN-ACK packets will prevent a TCP connection from being established. Jamming ARP-REQUEST or ARP-RESPONSE packets will prevent IP from associating IP and MAC addresses. Jamming a few protocol control packets can prevent or delay connections; preventing the connection when the goal is to shut the connection down and delaying the connection when the goal is to inhibit communication without being detected.

As suggested from the above, knowing which packet to jam is the key to getting significant jamming gains. A sensor needs to identify the key control packets from different protocols. Sensing can be online or offline. In online sensing packets are identified as they are received. This can be difficult since in some cases a packet is identified A size packets get clumped to the same size. It is assumed that none of these schemes has any significant effect on the timing of packets.

Figure 2: Exploiting multi-hop ad hoc routing. Ad hoc node A is communicating with C through B. The Sensor / Jammer identifies the target packet on the first hop and jams it on the second hop.

Field within a protocol sequence that has not yet completed. Offline sensing is allowed to classify packets received in the past based on packets received both before and after the packet in question. Off- line sensing is not directly useful for jamming. However, it can provide data that allows the attacker to better characterize the victim network and improve its online sensing. These jamming and sensing ideas are explored more in a later section.

Ad hoc networks add another protocol that can be attacked. Jamming A-RREQ or AODV-RREP packets will prevent ad hoc routes from ever being established. Ad hoc network protocols add additional packet types that can be detected. They also invoke mechanisms such as route request floods which can be exploited to glean network topology information. Jamming AODV-RREP packets can trigger additional packet floods that can cause network congestion. By the time a sensor classifies a packet it is too late to be jammed. Any jamming signal in response to online sensor classification would arrive after the packet is received by its intended receiver. This leads to the more significant role played by ad hoc networks. In a multi-hop path, a packet is transmitted and retransmitted several times. This provides an opportunity for a packet to be identified on one hop and jammed on the second hop. The attacker can either wait for the relayed packet or jam a sufficiently long time to account for variations in the forwarding times. Ad hoc networking could also support a network of attackers sharing sensing information and jamming attacks.

5 IMPLEMENTATION DETAILS

5.1 JAMMING PREVENTION

Together jamming and sensing can be broken down into a layered model similar to the OSI stack. We break it down into three levels for convenience as shown in Figure 1. The Link/Physical layer directly interacts with the media. If a higher layer requests a packet to be jammed, then this lower layer generates the physical signal and ensures that a packet and each of its link layer retries are jammed. This layer also provides the basic sensing capability of packet duration and timing. If sophisticated enough it could shield the upper layer from Link, MAC, and Physical layer control packets such as RTS/CTS and only report the higher OSI layer packets to the higher layer sensing and jamming.

The Transport/Network Layer interacts with the corresponding Ad Hoc, IP, TCP, and UDP protocols. This layer senses packet types and traffic flows which can then be targeted by jamming.

The Application layer senses HTTP sessions, VoIP set up and the like and targets specific user activities for jamming. It also sets higher level policies that define when jamming should take place and what targets in the victim network should be jammed. Example polices might be purely to sense the kind of network activity, to jam as surreptitiously as possible, or to prevent communications at any costs.

Each of these layers contributes to the overall performance of the system so that each layer can provide its own contribution to jamming gain, targeted jamming, and low probability of detection. This paper discusses exclusively the role of jamming at the Trans- port/Network layer. The Link/Physical layer provides a sensing and jamming service. The jamming service is defined as jamming for a specified period, jamming a specified number of packets,

or to start jamming continuously until a stop jamming request is made.

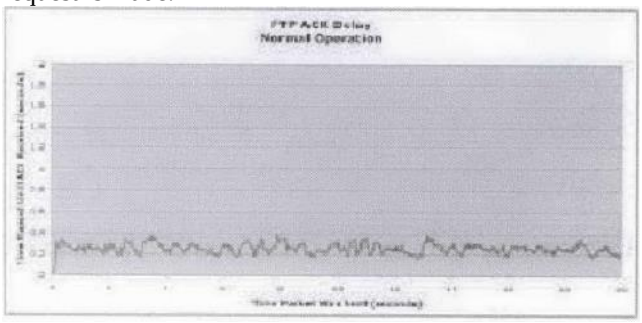

Fig.1 **Normal network conditions**

6 GENERIC ALGORITHM FOR SELECTIVE JAMMING ATTACK PREVENTION

S →jam receiver temp storage

Node → node pockets traffic

MAC → MAC address part

MAX → Method for sorting jam channel

N→ selective method with priority of channel

S (node, dest, MAC)

For each pocket to MAX MAC (m)

N (node) =MAX_m + MAC_m

IF node (α+ß (MAX (m)))

Else

Ignore MAX (N (pocket))

For Each CHANNEL to MAX (CHANNEL)

Repeat upto end End CHANNEL

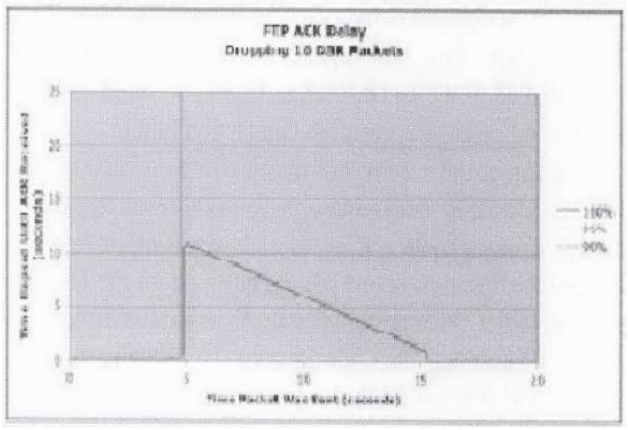

Fig.2 **Network conditions when jamming packets under various confidence intervals with generic algorithm**

7 SECURITY ISSUES

The attacks in this paper are based on carefully exploiting protocol patterns and consistencies across size, timing and sequence. This suggests that to make networks more secure these consistencies should be removed wherever possible. For size, padding control packets so that they are all the same size will make it difficult to discern different packet types. Padding all packets including control so that they have the same minimum size (say 100 bytes) will further remove size as useful metric. For wireless MAC protocols such as 802.11, every packet has substantial overhead so that small pack- ets already consist mostly of this overhead. Additional padding will have minimum effect on throughputs.

7.1 EVALUASTION OF PACKET-HIDING TECHNIQUES

In this section, we evaluate the impact of our packet-hiding techniques on the network performance via extensive simulations. We used the OPNET Modeler 14.5 [18] to implement the hiding sublayer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad hoc networks. We chose a set of nodes running 802.11b at the PHY and MAC layers, AODV for route discovery, and TCP at the transport layer. Aside from our methods, we also implemented a simple MAC layer encryption with a static key.

Timing in these protocols is overly precise. In TCP, the receiver does not use the three second back off time between the first and second TCP-SYN. Indeed, if the first one has been jammed it is not even expecting the second. Similarly, the precise timing between many packets in the sequence can be varied by significant factors so that it is difficult to precisely jam the packets. The timing of some the packets such as TCP-ACKs is used by protocols for estimating aspects of the network. But, it is conceivable that these protocols could be modified to allow for added delays. For instance, the header could indicate any additional delay that was added for security reasons so that this could be factored into RTT calculations.

Sequence for the protocols is immutable. But, it also can be foiled. One approach is to aggregate multiple packets. This will affect both timing and size of packets as well as potentially hiding the precise number of packets that are exchanged. Another attack is what we refer to as the zebra defence in which a single connection is striped across multiple TCP connections so that the attacker has difficulty separating and attacking individual victim connections.

Collectively, these approaches will make these networks more se- cure against the types of jamming attacks

described in this paper. It will be more difficult to discern and jam specific packet types. How-ever, the protocol information is not fully removed and other work has shown that longer sequence patterns can be classified with only coarse estimates of size and timing [22][23]. Further work is necessary to explore this exchange of measures and countermeasures.

CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine

Cryptographic primitives such as commitment schemes, Cryptographic puzzles and all-or-nothing transformations with physical-layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

[1] The Apache HTTP Server Project, release 2.0, downloaded Sep. 2004. http://httpd.apache.org/

[2] APE Project, How to build, install and run the APE tested, Uppsala University, Nov. 8, 2002
http://apetestbed.sourceforge.net/ape-testbed.pdf

[3] Bellardo, J., Savage, S., 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX Security Symposium, 2003.

[4] Bellovin, S.M., Probable plaintext cryptanalysis of the IP security protocols, In Proc. 1997 Symposium on Network and Distributed System Security. Feb. 1997 pp. 52–59

[5] Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N., Privacy vulnerabilities in encrypted HTTP streams, In Proc. Privacy Enhancing Technologies Workshop (PET 2005).

[6] Click Modular Router Project, MIT, release 1.4.3, downloaded Dec. 2004 http://pdos.csail.mit.edu/click/

[7] Fu, X., Graham, B., Bettati, R., Zhao, W. Active traffic analysis attacks and countermeasures. In Proc. of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[8] Gupta, V., Krishnamurthy, S., Faloutsos, M. Denial of service attacks at the MAC layer in wireless ad hoc networks. In Proc of Milcom, 2002.

[9] Hu, Y.-C., Perrig, A. A survey of secure wireless ad hoc rout-ing. IEEE Security & Privacy Magazine. v. 02, n. 3, (May-Jun-2004), pp. 28–39.

[10] Joncheray, L. A simple active attack against TCP. In Proc. Fifth Usenix UNIX Security Symposium, 1995

[11] Landeta, D., Secure Wireless LAN SecNet 11 & SecNet 54, in Information Assurance Solutions Working Symposium, Aug.2005. See also,
http://www.govcomm.harris.com/secure-comm/

[12] Perkins, C., Royer, E., Das, S., Ad hoc on-demand distance vector (AODV) routing, Internet Draft, draft-ietf-manet-aodv- 11.txt, work in progress, Aug 2002.

[13] Raymond, J. Traffic analysis: protocols, attacks, design issues and open problems. In H. Federrath, ed., Designing Privacy Enhancing Technologies, v. 2009 of LNCS, pp. 10–29.Springer-Verlag, 2001

[14] Stahlberg, M.. Radio jamming attacks against two popular mobile networks. In H. Lipmaa and H. Pehu-Lehtonen, ed., Proc. of the Helsinki University of Technology Seminar on Network Security. Fall 2000.

[15] Stallings, W., Wireless Communications and Networks, 2nd Ed., Prentice Hall, 2005.
[23] Wright, C.V., Monrose, F., Masson, G.M., Towards bette protocol identification using profile HMMs, JHU Technical Report JHU-SPAR051201, 14p., June, 2005.

[16] M K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook. McGraw-Hill, 2001.
.

[17] D. Stinson, “Something about All or Nothing (Transforms),”Designs, Codes and Cryptography, vol. 22, no. 2, pp. 133-138, 2001.

[18] D. Stinson, Cryptography: Theory and Practice. CRC press, 2006.

[19] M. Strasser, C. Popper, and S. Capkun, "Efficient Uncoordinated fish Anti-Jamming Communication," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 207-218, 2009.

[20] Sun, Q., Simon, D.R., Wang, Y., Russell, W., Padmanabhan V.N., Qiu, L., Statistical identification of encrypted web browsing traffic. IEEE Symposium on Security and Privacy,2002.

[21] Uppsala University, The Ad hoc Protocol Evaluation (APE) testbed, release 0.3, downloaded Nov. 2005 http://apetestbed.sourceforge.net

[22] Wright, C.V., Monrose, F., Masson, G.M., HMM profiles for network traffic classification (extended abstract), in Proc. ACM Workshop on Visualization and Data Mining for Computer Security, pp. 9–15, Oct. 2004.

[23] Wright, C.V., Monrose, F., Masson, G.M., Towards bette protocol identification using profile HMMs, JHU Technical Report JHU-SPAR051201, 14p., June, 2005.

[25] M K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

.

[26] D. Stinson, "Something about All or Nothing (Transforms),"Designs, Codes and Cryptography, vol. 22, no. 2, pp. 133-138, 2001.

[27] D. Stinson, Cryptography: Theory and Practice. CRC press, 2006.

[28] M. Strasser, C. Popper, and S. Capkun, "Efficient Uncoordinated fish Anti-Jamming Communication," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 207-218, 2009.

[29] M. Strasser, C. Popper, S. _Capkun, and M. Cagalj, "Jamming-Resistant Key Establishment Using n-coordinated Frequency Hopping," Proc. IEEE Symp. Security and Privacy, 2008.

[30] P. Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC), 2007.

[31] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

[32] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[33] D. Thuente and M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks," Proc. IEEE Military Comm. Conf. (MILCOM), 2006.

[34] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic Is the Threat," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[35] W. Xu, W. Trappe, and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Conf. Wireless Network Security (WiSec), pp. 203-213, 2008.

[36] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 46-57, 2005.

[37] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service," Proc. Third ACM Workshop Wireless Security, pp. 80-89, 2004.

