Classification Methods for Detecting Jamming Attacks

Suresh Bandi [1], Vakkalanka Venkata Syam [2]

[1]Student, AL-AMMER College of Engineering & Information Technology,Anandapuram,Visakapatnam.

[2]Assistant Professor, AL-AMMER College of Engineering & Information Technology,Anandapuram,Visakapatnam

Abstract: Adversary disrupts victim's communication channels through jamming in wireless ad hoc network governed by reactive protocols. Although the attack models are classified as both external and internal with the later being more serious because the “always-on” strategy employed in external model 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. In an internal threat model an adversary is assumed to be aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. Although RREQ,RREP,RERR, RREP-ACK are primary Message Formats in reactive protocols, the adversary selectively targets RREQ and RREP packets in the network to launch jamming attacks. Prior approaches concentrated on using commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the purview of the adversary. These approaches being successful, we propose to use them along with intrusion detection techniques for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure. A practical implementation validates our claim.

Keywords: Selective jamming, denial-of-service, wireless networks, packet classification.

 ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

I. INTRODUCTION

Jamming end-to-end transmissions in a wireless network [1] or underwater acoustic network [2] can have debilitating effects on data transport through the network. The effects of jamming at the physical layer resonate through the protocol stack, providing an effective denial-of-service (DoS) attack [3] on end-to-end data communication. The simplest methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beam forming, forcing

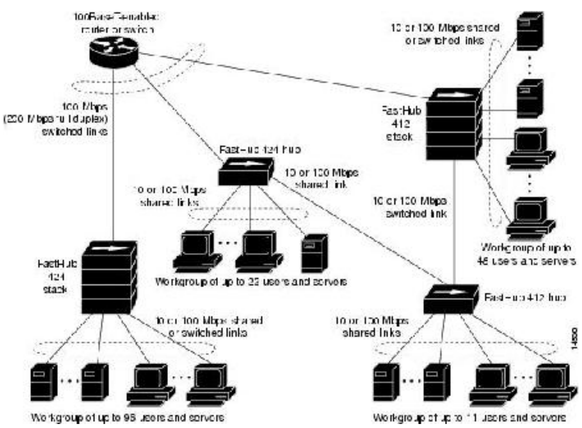

Fig 1: Architecture

The majority of anti-jamming techniques make use of diversity. For example, anti-jamming protocols may employ multiple frequency bands, different MAC channels, or multiple routing paths. Such diversity techniques help to curb the effects of the jamming attack by requiring the jammer to the jammers to expend a greater resource to reach the same goal. However, recent work has been done to demonstrate that intelligent jammers can incorporate cross layer protocol information into jamming attacks, reducing resource expenditure by several orders of magnitude by targeting certain link layer and MAC implementations [4]–[6] as well as link layer error detection and correction protocols [7]. Hence there are more number of anti-jamming measures have been taken into higher layer protocols. for example channel surfing or routing around jammed regions of the network [6].

act on multiple resources simultaneously. In this paper, we propose to use them along with intrusion detection techniques for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure. To make effective use of this routing diversity, however, each source node must be able to make an intelligent allocation of traffic across the available paths while considering the potential effect of jamming on the resulting data throughput.

In the existing system, We consider a sophisticated adversary who is aware of network secrets and the implementation

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

II. PROBLEM STATEMENT:

Uses Wireless networks. Packet Types involving in these networks are

1. Route Request (RREQ) Message Format
2. Route Reply (RREP) Message Format
3. Route Error (RERR) Message Format
4. Route Reply Acknowledgment (RREP-ACK) Message Format.

Fig 2: Jamming attack description with attacker node(using Rrep-Ack Rerr,Rrep,Rreq)

Jamming is not a transmit-only activity. It requires an ability to detect and identify victim network activity, which we denote as sensing. At the physical layer a sensor needs to identify the presence of packets. Since the network is encrypted, only the start time and size of the packet can be measured. At higher layers a sensor needs to classify packets using protocol information. In 802.11 for instance, whether a packet is successfully jammed or not can be seen by whether or not a node sends a short packet (i.e. the RREP-ACK) within 10msec.

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. 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

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

unusually high interference levels makes this type of attacks easy to detect.

Conventional anti jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). 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.

1. Fails to efficiently handle internal threat models.
2. So a better jamming detection system is required to handle internal threat models.

III. PROPOSED WORK:

Uses Wireless networks driven by reactive protocols containing RREQ, RREP, RERR, RREP-ACK message packets. Proposes to use commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the purview of the adversary.

Fig 3: Jamming Solution with hash key generator (using Rreq, Rrep, Rerr, Rrep-Ack)

A strong hiding commitment scheme, which is based on symmetric cryptography such as AES/DES is used to prevent selective jamming. A model that employs adversary filtration at the time of network joining though compromised routers is a better way of preventing jamming before it can actually happen. So a better system is required that implements this claim.

IV. OUR APPROACH:

Still uses Wireless networks driven by reactive protocols containing RREQ, RREP, RERR, RREP-ACK message packets. Proposes to use commitment schemes along with intrusion detection techniques for identifying compromised routers.

Fig 4: Router Rejected in our approach(In jamming there is no permissions)

This increases overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure. Offers an optimized network performance and security compared to prior systems.

V. RELATED WORK:

In the previous research, we have studied that the effect of the external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary exploits interpacket timing information to infer eminent packet transmissions. In [7], Law et al. proposed the estimation of the probability distribution of inter packet transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were predicted using estimated timing information. Using their model, the authors proposed selective jamming strategies for well-known sensor network MAC protocols.

Several researchers have suggested channel-selective jamming attacks, in which the jammer targets the broadcast control channel. It was shown that such attacks reduce the required power for performing a DoS attack by several orders of magnitude . To protect control-channel traffic, the replication of control transmission in multiple channels was suggested in , , [7]. The “locations” of the control channels were cryptographically protected. In [4],Lazos et al. proposed a randomized frequency hopping algorithm to protect the control channel from inside jammers. Strasser et al. proposed a frequency hopping antijamming technique that does not require the existence of a secret hopping sequence, shared between the communicating parties [6].

VI. CONCLUSION:

The problem identified is selective jamming. Adversary disrupts victim's communication channels through jamming in wireless ad hoc network governed by reactive protocols. Although the attack models are classified as both external and internal with the later being more serious because the “always-on” strategy employed in external model has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

continuous presence of unusually high interference levels makes this type of attacks easy to detect. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. Although RREQ, RREP, RERR, RREP-ACK are primary Message Formats in reactive protocols, the adversary selectively targets RREQ and RREP packets in the network to launch jamming attacks. Prior approaches concentrated on using commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the purview of the adversary. These approaches being successful, we propose to use them along with intrusion detection techniques for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure.

VII. REFERENCES:

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Computer Networks, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[2] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," IEEE Journal of Oceanic Engineering, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[3] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. JohnWiley&Sons, Inc.,2001.

[4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symposium, Washington, DC, Aug. 2003, pp. 15–28.

[5] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06), Washington, DC, Oct. 2006, pp. 1–7.

[6] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs," Wireless Communications and Mobile Computing, vol. 5, no. 3, pp. 273–284, May 2005.