Resilient Multi-Path Routing and Hiding Packets for Preventing Selective Jamming Attacks

Manoj Kumar M
Dept. of ISE, YDIT

Sakhib Quarishi
Dept. of ISE, YDIT

Syed Yousuf
Dept. of ISE, YDIT

Mrs. P. Soubhagyalakshmi,
Associ. Prof. Dept. of CSE, YDIT

***Abstract*— In this paper, the intruder is functional only for a short duration of time span, selectively targeting messages containing data of high importance. We emphasize the benefits of selective jamming in terms of network performance degradation and an intruder attacks by presenting two cases ; a selective strike on TCP and routing. We demonstrate that selective jamming attacks can be organized by accomplishing real-time packet classification done at the physical layer. To overcome these attacks, we provide three schemes that avoid real-time packet classification by combining cryptographic primitives with physical-layer properties. We examine the security of our methods and evaluate its computational and communication overhead. We examine jamming at the network level and focus on replacing the end-to-end data delivery through multipath routing. As long as all paths do not fail concurrently, the end-to-end path availability is maintained. The multipath selection upgrades routing by choosing node-disjoint paths or link-disjoint paths. We show that topological disjointness is insufficient for selecting fault- independent paths. Thus, we address multipath selection based on the knowledge of a path's *availability history*. Using Availability History Vectors (AHVs) of paths, we present an AHV-based Link-State (ALS) algorithm to select fault- independent paths.**

Keyword — Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification, Reliability, Security, Routing algorithms.

I. INTRODUCTION

In this paper, we address the problem of jamming under an internal threat model. We consider an adversary who is known of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary misuses his/her internal knowledge for performing *selective jamming attacks* in which certain messages of "high importance" are chosen. For example, a jammer can attack route-request/route-reply messages at the routing layer to disable route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To perform selective jamming attacks, the adversary must be skilled of implementing a "classify-then-jam" strategy before the fulfillment of a wireless transmission. Such plans can be actualized either by systemize transmitted packets using protocol semantics [1] or by decrypt packets on the fly. In the final method, the jammer may decode the first few bits of a packet for obtaining useful packet identifiers such as packet type, source and destination address. After classification, the adversary must actuate a sufficient number of bit errors so that the packet cannot be received at the receiver. Selective jamming needs an intimate knowledge of the physical layer, as well as of the specification of upper layers. We also examine multipath routing protocols that will react to communication disturbance on-demand. Particularly, a source node which selects multiple paths to reach the destination. When one of the paths fades, other working paths will be used to deliver packets and maintain end-to-end availability, *as long as not all paths between the source and destination fail concurrently*. Such end-to-end availability is provided by multiple paths between a pair of nodes which is named as *multipath availability*. A crucial component of multipath routing is *multipath selection*, as the selection logic and resulting path qualities will directly impact the effectiveness of multipath routing. In this study, we design multipath selection algorithms that modify multipath availability even when one or more jammers make a mess of network communication occasionally or continuously.

Most existing multipath selection algorithms [4, 9] choose node-disjoint paths or link-disjoint paths, i.e., paths without common nodes or shared links, in a venture to minimize the probability that paths fail simultaneously. While such an approach is simple and accurate, it depends upon the assumption that the topological disjointness among multiple paths is sufficient to guarantee failure-independence. But in a wireless network, disjoint paths can still be failure-correlated, especially in the presence of multiple interference sources. To address the failure correlation between disjoint paths in the presence of jamming, one way is to mathematically model the effects of jamming on the network links. However, electromagnetic signals propagate in complex environments full of absorption, reflection, scattering and diffraction and the resulting jamming impact on the network is highly irregular [2].

II. RELATED WORKS

Jamming attacks on voice communications have been started since the 1940s. In the context of digital communications, the jamming problem has been addressed under various threat models. We present a classification based on the selective nature of the adversary.

A. Prior work on Selective Jamming

We study the impact of an external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary utilizes inter-packet timing information to conclude eminent packet transmissions. In [11], Law et al. proposed the evaluation of the probability distribution of inter-packet transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were analyzed using estimated timing information. Using their model, the authors proposed selective jamming strategies for well known sensor network

MAC protocols. In [1], Brown et al. illustrated the feasibility of selective jamming based on protocol semantics. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of different protocols, and physical signal sensing. To prevent selectivity, the unification of packet characteristics such as the minimum length and inter-packet timing was proposed. Similar packet classification techniques were investigated in [4].

Liu et al. considered a smart jammer that takes into consideration of protocol specifics to optimize its jamming strategy. The adversary was imagined to target control messages at different layers of the network stack. To reduce smart jamming, the authors proposed the SPREAD system, which is based on the idea of stochastic selection between a collection of parallel protocols at each layer. The uncertainty introduced by this stochastic selection, mitigated the selective ability of the jammer. Greenstein et al. presented an 802.11-like wireless protocol called Slyfi. It prevents the classification of packets by external observers. This protocol hides all explicit identifies from the transmitted packets (e.g. MAC layer header and payload), by encrypting them with keys only known to the intended receivers [8].

Selective jamming attacks have been experimentally implemented using software-defined radio engines. Wilhelm et al. implemented a USRP2-based jamming platform called RFReact that permits selective and reactive jamming. RFReact was shown to be doubter to technological standards and are adaptable to any required jamming strategy. The success rate of a selective jamming attack against a 802.15.4 network was measured to be 99.96%. They showed that a selective jammer targeting specific packets in a point-to-point 802.11 communication was able to reduce the rate of the communication to the minimum value of 1 Mbps, with relatively little effort (jamming of 5-8 packets per second). The results were experimentally checked using the USRP2/GNU radio platform.

Several researchers have suggested channel-selective jamming attacks, in which the jammer attacks the broadcast control channel. It was shown that such attacks reduce the required power for performing a DoS attack by several orders of magnitude [3]. To protect control-channel traffic, the duplication of control transmission in multiple channels was suggested in [3], the "locations" of the control channels were cryptographically protected. In [12], Lazos et al. proposed a randomized frequency hopping algorithm to protect the control channel from inside jammers. Strasser et al. proposed a frequency hopping anti-jamming technique that does not require the existence of a secret hopping sequence, shared between the communicating parties.

B. Non-Selective Jamming Attacks

Conventional methods for reducing jamming employ some form of SS communications [5]. The transmitted signal is spread to a larger BW following a PN sequence. Without the knowledge of this sequence, a large amount of energy (typically 20-30 dB gain) is required to interfere with an ongoing transmission. However, in the case of broadcast communications, accommodation of commonly shared PN codes neutralizes the advantages of SS.

Poopperetal proposed a jamming-resistant communication model for pair wise communications that does not rely on shared secrets. Communicating nodes use a physical layer modulation method called Uncoordinated Direct-Sequence Spread Spectrum (UDSSS). They also proposed a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a public codebook. Several other schemes eliminate overall the need for secret PN codes.

Lin et al. showed that jamming 13% of a packet is sufficient to overcome the ECC capabilities of the receiver [13]. Xu et al. categorized jammers into four models: (a) a constant jammer, (b) a deceptive jammer that broadcasts fabricated messages, (c) a random jammer, and (d) a reactive jammer that jams only if activity is sensed. Cagalj et al. proposed wormhole-based anti- jamming techniques for wireless sensor networks (WSNs) [2]. Using a wormhole link, sensors within the jammed region establish communications with outside nodes, and notify those regarding ongoing jamming attacks.

III. ASSUMPTIONS

Problem Statement

Consider the scenario where 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 aim is to transform a selective jammer to a random one. In the current work, we do not address packet classification methods based on protocol semantics, as described in [1], [4], [11].

System and Adversary Model

Network model–The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pair wise keys or asymmetric cryptography.

Communication Model–Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries $^{\alpha}q$ data bits, where α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is $^{\alpha}q$R bps. Spread spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmissions from jamming. SS provides immunity to interference to some extent (typically

20 to 30 dB gain), but a powerful jammer is still capable of jamming data packets of his/her choosing.

The preamble is used for synchronizing the sampling process at the receiver. The PHY layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination addresses, sequence numbers and some additional fields. The MAC header is followed by the frame body that typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.

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 (similar to the Dolev-Yao model). The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of multi-radio transceivers. 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. For analysis purposes, we assume that the adversary can pro-actively jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the *last symbol*. In reality, it has been demonstrated that selective jamming can be achieved with far less resources. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent adversary that can be effective even at high transmission speeds.

The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard crypto- graphic problems is assumed to be time-consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space.

The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may operate unattended, thus being susceptible to physical compromise.

IV. AHV-BASED LINK-STATE ALGORITHM

The success of multipath selection necessitates two components, namely, (a) a *metric* that can accurately reflect failure correlation between different paths, and (b) a *selection algorithm* that effectively leverage metric to rule out failure-correlated paths from being selected together.

AHV Select: AHV-Based Multipath Selection

a) Require: INPUT: H, k, {Ai} i∈ H

OUTPUT: ***M;***
PROCEDURES:
1: M = Ø, θ (M) = 0
2: while |M| ≤ k do
3: select a path p ∈H that maximizes θ (M ∪p)
4: add p to M, update θ (M) = θ (M ∪p)
5: end while

V. CONCLUSIONS

In this paper, we addressed the problem of multipath selection with the goal of improving jamming resilience in wireless networks. Our key insight is to select multiple paths that are likely to fail concurrently, based on the knowledge of paths availability histories, the available histories of path are efficiently recorded and calculated via availability history vectors (AHVs). Levering AHVs we have presented AHVs-based link –state multipath selection algorithms. Our extensive simulation results have validated that

1. Selecting disjoint paths is insufficient to improve end-to-end availability in the presence of jamming.
2. AHVs based algorithms can efficiently identify multipath that provide high end to end availability even in the presence of new jammer that has not yet affected the AHVs prior to path selection.

In summary, our AHV-based algorithms can greatly improve the end-to-end message delivery in the presence of a wide variety of jamming attacks.

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 (AONTs) with physical layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

[1] 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.
[2] R. D. Binns, D. Millard, and L. Harris,"Data havens, or privacy sans frontieres?: a study of international personal data transfers," in Proc. of the ACM conference on Web science (WebSci), 2014, pp. 273–274.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In *Proceedings of ISIT*, 2007.

[4] 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.

[5] Y. Desmedt. Broadcast anti-jamming systems. *Computer Networks*, 35(2-3):223–236, February 2001.

[6] L. Zeng, Z. Shi, S. Xu, and D. Feng, "Safevanish: An improved data self-destruction for protecting data privacy," in Proc. of the Second International Conference on Cloud Computing Technology and Science (CloudCom), Indianapolis, IN, Dec. 2010, pp. 521–528.

[7] L. Zeng, S. Chen, Q. Wei, and D. Feng, "SeDas: A self-destructing data system based on active storage framework," IEEE Transactions on Magnetics, vol. 49, no. 6, pp. 2548–2554, 2013.

[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 Sensors 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 2nd ACM conference on wireless network security*, pages 169–180, 2009.

[10] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. *Wireless Communications and Mobile Computing*, 5(3):273–284, May 2004.

[11] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In *Proceedings of INFOCOM*, pages 2536–2540, 2007.

[12] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *Proceedings of INFOCOM*, San Diego, 2010.

[13] C. Po¨pper, M. Strasser, and S. Cˇ apkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the USENIX Security Symposium*, 2009.