ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

Avoidance of Discerning Jamming Attacks Using Packet Thrashing Methods

J.Vadivambigai, S.Arul Antran Vijay[2], Chinthuramdas

Assistant Professor, Department of CSE, Karpagam College of Engineering, Coimbatore, India [1,2,3]

ABSTRACT: The open nature of the wireless medium leaves it susceptible to intentional interference attacks, classically referred to as jamming, This intentional interference with wireless transmissions can be used as a launch pad for rising Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to perceive and counter. In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the jammer selectively targeting messages of high importance. We demonstrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and the second case study is on routing. We show those selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. We analyze the security of our methods and appraise their computational and communication overhead.

KEYWORDS: Selective Jamming, Denial-of-Service, Wireless Networks,

I. INTRODUCTION

Wireless networks rely on the continuous availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it susceptible to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject fake messages, or jam legal ones. While eavesdropping and message injection can be prohibited 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]. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses . 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 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. 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. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is 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. 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. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics [1]by decoding packets on the fly . In the latter method, the jammer may decode the first few bits of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver . Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

Our Contributions–We investigate the feasibility of realtime packet classification for launching selective jamming attacks, under an internal threat model. We show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. We investigate the impact of selective jamming on critical network functions. Our findings indicate that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer. To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

II. PROBLEM STATEMENT AND ASSUMPTIONS

2.1 *Problem Statement*

Consider the scenario depicted in Fig. 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].

2.2 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 preshared 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 q data bits, were α/β is the rate of the PHY-layer encoder. 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, but a powerful jammer is still capable of jamming data packets of his choosing. Transmitted packets have the generic format depicted in Fig. 1(b). 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 plus 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,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

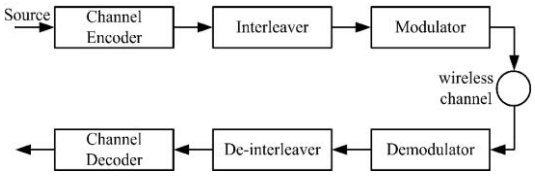
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

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 cryptographic problems is assumed to be time-consuming.

III. REAL-TIMEPACKET CLASSIFICATION

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m.



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.

IV. IMPACT OF SELECTIVE JAMMING

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNETTM Modeler 14.5 to implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

Selective Jamming at the Transport Layer–In the first set of experiments, we setup a file transfer of a 3 MB file between two users A and B connected via a multi-hop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection.

Selective Jamming at the Network Layer–In this scenario, we simulated a multi-hop wireless network of 35 nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam non-overlapping areas of the network. Three types of jamming strategies were considered: (a) a continuous jammer, (b) a random jammer blocking only a fraction p of the transmitted packets, and (c) a selective jammer targeting route request (RREQ) packets.

V. HIDING BASED ON COMMITMENTS

In this section, we show that the problem of real-time packet classification can be mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments.

5.1 Mapping to Commitment Schemes

Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V while keeping m hidden. H*iding:* For every polynomial-time party V interacting with A, there is no polynomially-efficient algorithm that would allow V to associate C with m and C′ with m′, without access to the recommitment values d or d′ respectively, and with non-negligible probability. B*inding:* For every polynomial-time party A interacting with V , there is no polynomially efficient algorithm that would allow A to generate a triple (C, d, d′), such that V accepts the commitments (C, d) and (C, d′), with non-negligible probability.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

5.2 A Strong Hiding Commitment Scheme (SHCS)

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. Assume that the sender S has a packet m for R.S constructs (C,d)= commit(m), where, C = Ek(π1(m)), d = k. C = Ek(π1(m)), d = k.

5.3 Implementation Details of SHCS

The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead of SHCS, the recommitment value d (i.e., the decryption key k) is carried in the same packet as the committed value C. This saves the extra packet header needed for transmitting d individually. To achieve the strong hiding property, a sub layer called the "hiding sub layer" is inserted between the MAC and the PHY layer. This sub layer is responsible for formatting m before it is processed by the PHY layer.

5.4 Security Analysis

In this section, we analyze the security of SHCS by evaluating the ability of J in classifying a transmitted packet at different stages of the packet transmission. **Release of** C–We first examine if J can classify m by observing the commitment value C. Though C and k are part of the same packet, symbols corresponding to C are received first. The jammer can attempt to classify m by launching a cipher text-only attack on C as early as the reception of the first cipher text block. Because the encryption key is refreshed at every transmission, a very small number of cipher text blocks are available for cryptanalysis. Appropriate selection of the key length s can prevent this type of attack. Note that s can be well below the cryptographic standards, due to the limited time available to the adversary (until the transmission is completed). For instance, a 56-bit long DES key is more than adequate for our purposes, since the fastest known brute force attack on DES takes almost a day . Other types of known attacks such as differential and linear cryptanalysis are not applicable, because they require the collection of a large number of chosen or known plaintext/cipher text pairs.

VI. HIDING BASED ON CRYPTOGRAPHIC PUZZLES

In this section, we present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver [10]. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead.

6.1 Cryptographic Puzzle Hiding Scheme (CPHS)

Let a sender S have a packet m for transmission. The sender selects a random key k ∈ {0, 1}s, of a desired length. S generates a puzzle P = puzzle(k, tp), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter tp is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second. After generating the puzzle P, the sender broadcasts (C, P), where C = Ek(π1(m)). At the receiver side, any receiver R solves the received puzzle P′ to recover key k′ and then computes m′ = π−1(Dk′ (C′)). If
the decrypted packet m′ is meaningful (i.e) is in the proper format, has a valid CRC code, and is within the context of the receiver's communication), the receiver accepts that m′ = m. Else, the receiver discards m′.

VII.AN AONT-BASED HIDING SCHEME (AONT-HS)

In our context, packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, . . . ,mx}, which serve as an input to an AONT f : {Fu}x → {Fu}x′ . Here, Fu denotes the alphabet of blocks mi and x′ denotes the number of output pseudo-messages with x′ ≥ x. The set of pseudo-messages m′ = {m′ 1, . . . ,m′ x′} is transmitted over the wireless medium. At the receiver, the inverse transformation f−1 is applied after all x′ pseudo-messages are received, in order to recover m.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

VIII. EVALUATION 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 OPNETTM Modeler 14.5 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.

Impact on real-time systems–Our packet-hiding methods require the processing of each individual packet by the hiding sublayer. We emphasize that the incurred processing delay is acceptable, even for real-time applications. The SCHS requires the application of two permutations and one symmetric encryption at the sender, while the inverse operations have to be performed at the receiver. Such operations can be implemented in hardware very efficiently. Symmetric encryption such as AES can be implemented at speeds of tens of Gbps/s when realized with Application Specific Integrated Circuits (ASICs) or Field Programmable Gate Arrays (FPGAs) [6]. These processing speeds are orders of magnitude higher than the transmission speeds of most current wireless technologies, and hence, do not impose a significant delay. Similarly, the AONT-HS performs linear operations on the packet that can be efficiently implemented in hardware. We note that a non-negligible processing delay is incurred by the CPHS. This is due to the cryptographic puzzle that must be solved at the receiver. As suggested in Section 6, CPHS should only be employed when the symbol size at the PHY layer is too small to support the SHCS and AONTHS solutions. The processing delays of the various schemes are taken into account in our experimental evaluations.

Experimental evaluation–In the first set of experiments, we setup a single file transfer between a client and server, connected via a multi-hop route. The client requested a 1 MB file from the server. We evaluated the effects of packet hiding by measuring the effective throughput of the TCP connection in the following scenarios: (a) No packet hiding (N.H.), (b) MAC-layer encryption with a static key (M.E.), (c) SHCS (C.S.), (d) Time-lock CPHS (T.P.), (e) Hash-based CPHS (H.P.), (f) Linear AONT-HS (L.T.), and (g) AONT-HS based on the package transform (P.T.).

IX. RELATED WORK

Jamming attacks on voice communications have been launched 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.

X. 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 (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] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. *IEEE Transactions on Mobile Computing*, 6(1):100–114, 2007.
[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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2013

[6] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. *Cryptographic Engineering*, pages 235–294, 2009.
[7] O. Goldreich. *Foundations of cryptography: Basic applications*. Cambridge University Press, 2004.
[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall Improving wireless privacy with an identifier-free link layer protocol. In *Proceedings of MobiSys*, 2008.
[9] IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/ download/802.11-2007.pdf, 2007.
[10] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Proceedings of NDSS*, pages 151–165, 1999.
[11] 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. *ACMTransactions on Sensors Networks*, 5(1):1–38, 2009.
[12] 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.
[13] 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.
[14] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In *Proceedings of INFOCOM*, pages 2536– 2540, 2007.
[15] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *Proceedings of INFOCOM*, San Diego, 2010.
[16] R. C. Merkle. Secure communications over insecure channels. *Com-munications of the ACM*, 21(4):294–299, 1978.