Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Prevention of Selective Jamming Attacks by using Packet – Hiding Methods

Khaja Ziauddin
Dept. of Computer Science and Engg.
& JNT University, India

Majoju Sridhar Kumar
Dept. of Computer Science and Engg.
& JNT University, India

Abstract: - Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect with participating nodes in ad hoc networks. This open nature of the wireless medium creates the chances of intentional interference attacks, typically referred to as jamming. And this jamming leads to Wireless Denial of Service (DoS) . Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. The adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. 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. Adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter.In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate 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 one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer.

Keywords: Ad hoc networks, wireless networks, jamming, cryptography, Denial of Service (DoS)

I. INTRODUCTION

Congestion in point-to-point transmissions in a wireless mesh network 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 on end-to-end data communication. 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.

The simplest methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beam forming, forcing the jammers to expend a greater resource to reach the same goal. However, recent work has demonstrated 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 as well as link layer error detection and correction protocols. The majority of anti- jamming techniques make use of diversity. In this project, we consider the anti-jamming diversity based on the use of multiple routing paths. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) or Ad-Hoc On-Demand Distance Vector (AODV) each source node can request several routing paths to the destination node for concurrent use. 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.

Our contributions to this problem are as follows:

1. We formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem. We map the optimization problem to that of asset allocation using portfolio selection theory.
2. We formulate the centralized traffic allocation problem for multiple source nodes as a convex optimization problem.
3. We show that the multi-source multiple-path optimal traffic allocation can be computed at the source nodes using a distributed algorithm based on decomposition in network utility maximization.
4. We propose methods which allow individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

II. PROBLEM STATEMENT

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 , or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of 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.

III. SELECTIVE JAMMING ATTACKS

3.1 Prior work on Selective Jamming

Thuente studied the impact of an external selective jammer who targets various control packets at theMAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions. 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 formation. Using their model, the authors proposed selective jamming a strategies for well known sensor network MAC protocols. 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.

3.2 Non-Selective Jamming Attacks

Conventional methods for mitigating jamming employ some form of SS communications. The transmitted signal is spread to a larger bandwidth 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, compromise of commonly shared PN codes neutralizes the advantages of SS. 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. They further studied the problem of detecting the presence of jammers by measuring performance metrics such as packet delivery ratio. Cagalj et al. proposed wormhole-based anti jamming techniques for wireless sensor networks (WSNs). Using a wormhole link, sensors within the jammed region establish communications with outside nodes, and notify them regarding ongoing jamming attacks.

3.3 Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks

WMNs follow a two-tier network architecture .The first tier consists of the end users, also referred to as stations (STAs), directly connected to mesh nodes, referred to as Mesh Access Points (MAPs). The second tier consists of a peer-to-peer network of the MAPs. Connectivity in the second tier is assisted by intermediate routers known as Mesh Points (MPs) which interconnect MAPs (MPs do not accept connections from end users).The network of MAPs and MPs is often static and uses separate frequency bands to communicate data and control information (MAPs are typically equipped with multiple transceivers). Finally, Mesh Gateways (MGs) provide connectivity to the wired infrastructure. An example of a WMN is shown in Fig.3.1

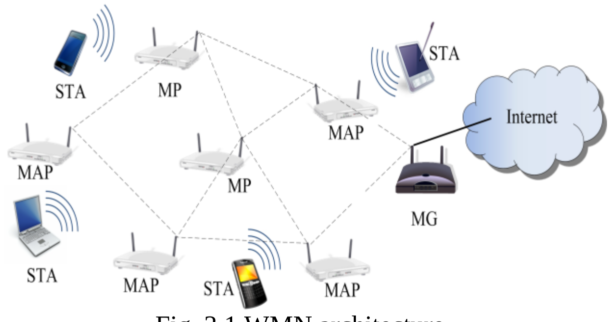

Fig. 3.1 WMN architecture.

WMNs are invariably vulnerable to "external" and "internal" attacks. External attacks take the forms of random channel jamming, packet replay, and packet fabrication and are launched by "foreign" devices that are unaware of the network secrets (e.g., cryptographic credentials and pseudo-random spreading codes). They are relatively easier to counter through a combination of cryptography based and robust communication techniques.

3.3.1 Selective Jamming Attacks

The open nature of the wireless medium leaves it vulnerable to jamming attacks. Jamming in wireless networks has been primarily analyzed under an external adversarial model, as a severe form of denial of service (DoS) against the PHY layer. Existing anti-jamming strategies employ some form of spread spectrum (SS) communication, in which the signal is spread across a large bandwidth according to a pseudo-noise (PN) code. However, SS can protect wireless communications only to the extent that the PN codes remain secret. Insiders with knowledge of the commonly shared PN codes can still launch jamming attacks. Using their knowledge of the protocols specifics, they can selectively target particular Channels/layers/protocols/packets. We describe two types of selective jamming attacks against WMNs, which employ channel and data selectivity.

A. Channel-Selective Jamming

In a typical WMN, one or more channels are reserved for broadcasting control information. These channels, referred to as control channels, facilitate operations such as network discovery, time synchronization, coordination of shared medium access, routing path discovery and others, without interfering with the communications of STAs with MAPs. An adversary who selectively targets the control channels can efficiently launch a DoS attack with a fairly limited amount of resources (control traffic is low-rate compared to data traffic). To launch a channel selective jamming attack, the adversary must be aware of the location of the targeted channel, whether defined by a separate frequency band, timeslot, or PN code. Note that control channels are inherently broadcast and hence, every intended receiver must be aware of the secrets used to protect the transmission of control packets. The compromise of a single receiver, be it a MAP or an MP, reveals those secrets to the adversary. Example: We illustrate the impact of channel selective jamming on CSMA/CA-based medium access control (MAC) protocols for multi-channel WMNs. A multi-channel MAC (MMAC) protocol is employed to coordinate access of multiple nodes residing in the same collision domain to the common set of channels. A class of MMAC protocols proposed for ad hoc networks such as WMNs follows a split-phase design (e.g., [5]). In this design, time is split into alternating control and data transmission phases. During the control phase, every node converges to a default channel to negotiate the channel assignment. In the data transmission phase, devices switch to the agreed on channels to perform data transmissions.

B. Data-Selective Jamming

To further improve the energy efficiency of selective jamming and reduce the risk of detection, an inside attacker can exercise a greater degree of selectivity by targeting specific packets of high importance. One way of launching a data-selective jamming attack, is by classifying packets before their transmission is completed. An example of this attack is shown in Fig. 3.3.2(a)

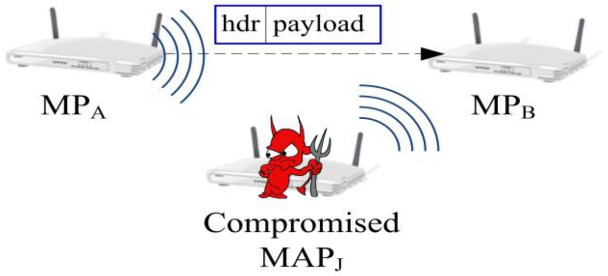

Fig. 3.3.1(a) A data-selective jamming attack

MPA transmits a packet to MPB. Inside attacker MAPJ classifies the transmitted packet after overhearing its first few bytes. MAPJ then interferes with the reception of the rest of the packet at MPB: Referring to the generic packet format in Fig. 3.3.2(b)

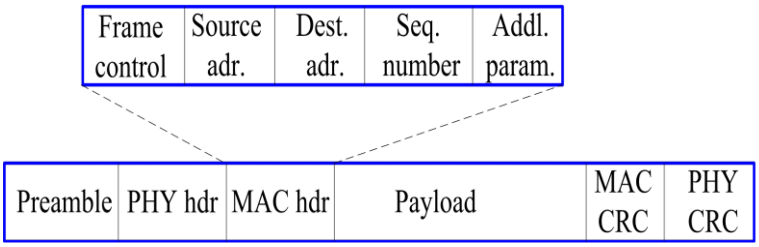

Fig 3.3.1(b)generic packet format

A packet can be classified based on the headers of various layers. For example, the MAC header typically contains information about the next hop and the packet type. The TCP header reveals the end-to-end source and destination nodes, the transport-layer packet type (SYN,ACK, DATA, etc.), and other TCP parameters.Another method for packet classification is to anticipatea transmission based on protocol semantics. Routing isperformed at the MAC layer according to the Hybrid Wireless Mesh Protocol (HWMP). The latter is a combinationof tree-based routing, and on-demand routing based on AODV. Tree-based routing provides fixed path routes from the mesh nodes to the MGs.

IV. SYSTEM ARCHITECTURE

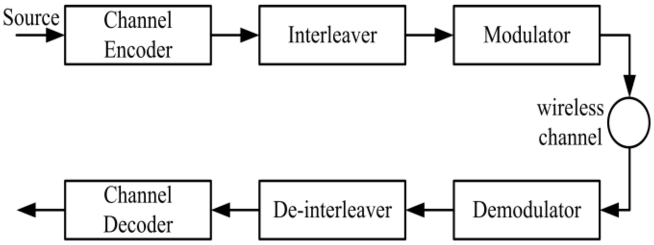

Fig. A generic communication system diagram.

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, DE interleaved, and decoded, to recover the original packet m. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

V. 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. The advantage of the puzzlebased scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

Sender*S* *Receiver R*

generate: *k*, *tp* $\xrightarrow{C,P \qquad C',P'}$

compute *k'* = *solve*(*P*)
P=*puzzle*(*k*,*tp*) compute: *m'* = *!*1-1(*Dk'*(*C'*))
C=*Ek*(*!*1(*m*)) verify: *m'* is meaningful
if not: discard *m'*

Fig. The cryptographic puzzle-based hiding scheme

In our context, we use cryptographic puzzles to temporary hide transmitted packets. A packet m is encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

5.1 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′. Fig.4.3 shows the details of CPHS.

VI. HIDING BASED ON ALL-OR-NOTHING TRANSFORMATIONS

In this section, we propose a solution based on All-Or- Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformationswere originally proposed by Rivest to slow down brute force attacks against block encryption algorithms.An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f, mapping message m = {m1, · · · ,mx} to asequence of pseudo-messages m′ = {m′1, · · · ,m′x′}, is an AONT if : (a) f is a bijection, (b) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo-messages is unknown, and (c) f and its inverse f−1 are efficiently computable. When a plaintext is pre-processed by an AONT before encryption, all ciphertext blocks must be received to obtain any part of the plaintext. Therefore, brute force attacks are slowed down by a factor equal to the number of ciphertext blocks, without any change on the size of the secret key.

*6.1 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.

Sender *S* **Receiver *R***
compute:
m || **pad**(*m*)
transform:
m' = *f* (*m* || **pad**(*m*)) m → receive *m*'
compute
m || **pad**(*m*)= *f -1*(*m*')
recover *m*

The AONT-based Hiding Scheme (AONT-HS)

VII. 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.

[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.IEEE802.11standard. 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.*