TO ALLEVIATE SELECTIVE JAMMING ATTACKS IN WIRLESS NETWORK BY USING PACKET HIDING SCHEMES

KEYWORDS

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

S. ARAVINDH

Associate ProfessorComputer Science and Engineering, Gojan School of Business and Technology,
80 Feet Road, Edapalayam, Red hills, Chennai-600 052, Tamilnadu, India

ABSTRACT Due to their open and ubiquitous nature, wireless information systems are extremely vulnerable to attack and misuse. Wireless systems can be attacked in various ways, depending on the objectives and capabilities of an adversary. Due to high availability and relatively low cost of powerful antennas, jamming, i.e., the use of active signals to prevent data distribution has emerged as an attractive way of attack. Jamming can be viewed as a form of Denial-of-Service (DoS) attack, whose goal is to prevent users from receiving timely and adequate information. 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 detect and counter. Proposed system focuses on internal threat model, address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. To thwart these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.

I. 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. 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 ant 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 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.

JAMMING ATTACKS

There are many different attack strategies an adversary can use to jam wireless communications

Constant jammer: The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal [7] or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette [4]. Normally, the underlying MAC protocol allows legitimate nodes to send out packets only if the channel is idle. Thus, a constant jammer can effectively prevent legitimate traffic sources from getting hold of a channel and sending packets.

Deceptive jammer: Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected.

Random jammer: Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a "sleeping" mode. It will resume jamming after sleeping for some time. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

Reactive jammer: The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. As we shall see in the following section, these methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.

II. PROBLEM STATEMENT

Consider the scenario depicted in Fig. 1. 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.

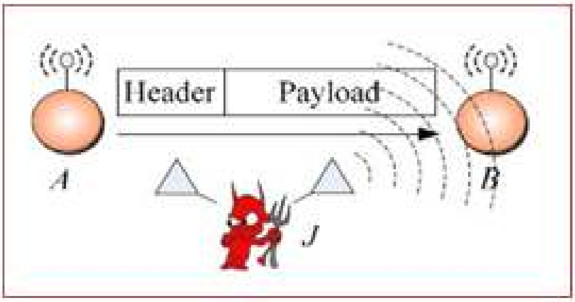

Fig. 1 Selective Jamming attack

III. REAL-TIME PACKET CLASSIFICATIONS

In this section, we describe how the adversary can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted in Fig. 2. 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, deinterleaved, and

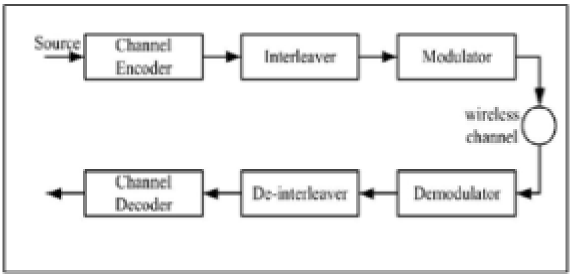

Fig. 2 Generic communication system

The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 2. The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors. One solution to the key compromise problem would be to update the static key whenever it is compromised. However, such a solution is not useful if the compromised node obtains the new key. This can only be avoided if there is a mechanism by which the set of compromised nodes can be identified. Such a task is nontrivial when the leaked key is shared by multiple nodes. Any node that possesses the shared key is a candidate malicious node. 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.

IV. SYSTEM ANALYSIS

A. EXISTING SYSTEM

Spread spectrum techniques have been used as countermeasures against jamming attacks. Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Chirp Spread Spectrum (CSS) are three common forms of spread spectrum techniques. In classic spread spectrum techniques, senders and receivers need to pre-share a secret key, with which they can generate identical hopping patterns, spreading codes, or timing of pulses for communication. However, if a jammer knows the secret key, the jammer can easily jam the communication by following the hopping patterns, spreading codes, or timing of pulses used by the sender. There have been a few recent attempts to remove the dependency of jamming-resistant communications on pre shared keys. Frequency Hopping (UFH) technique to allow two nodes that do not have any common secret to establish a secret key for future FHSS communication in presence of a jammer. These works successfully remove the requirement of pre-shared keys in point-to-point FHSS communication. Unfortunately, UFH and its variations cannot be directly used for broadcast communication, since their primary objective is to establish a pair wise key between two parties. Indeed, any spread spectrum communication system that requires a shared key, either pre-shared or established at the initial stage of the communication, cannot be used for broadcast communication where there may be insider jammers. Any malicious receiver, who knows the shared key, may use the key to jam the communication. To address this problem, researchers recently investigated how to enable jamming-resistant broadcast communication without shared keys

B. PROPOSED SYSTEM

The proposed system uses a packet hiding methods which is highly adaptive to prevent selective jamming attacks. The schemes used in this paper are distributed adaptive mechanism for impeding attackers' efforts to deny service to legitimate receivers. The level of protection employed by the sender is that they dynamically adjust to the current level of attack rates.
Thus the main aim of the proposed system is to hide the packet from jammers. This helps to reduce the selective jamming attacks and also DoS attacks in wireless networks.

C. SYSTEM ARCHITECTURE

Sender sends data in packets to receiver. The jammer jams the networks by eavesdropping the packets, adds information and introduces DoS attacks in wireless networks. The sender prevents packet by using three packet hiding mechanisms were proposed. Using these security schemes selective jamming attacks in wireless networks is prevented.Fig.3 represents overall system architecture for proposed system.

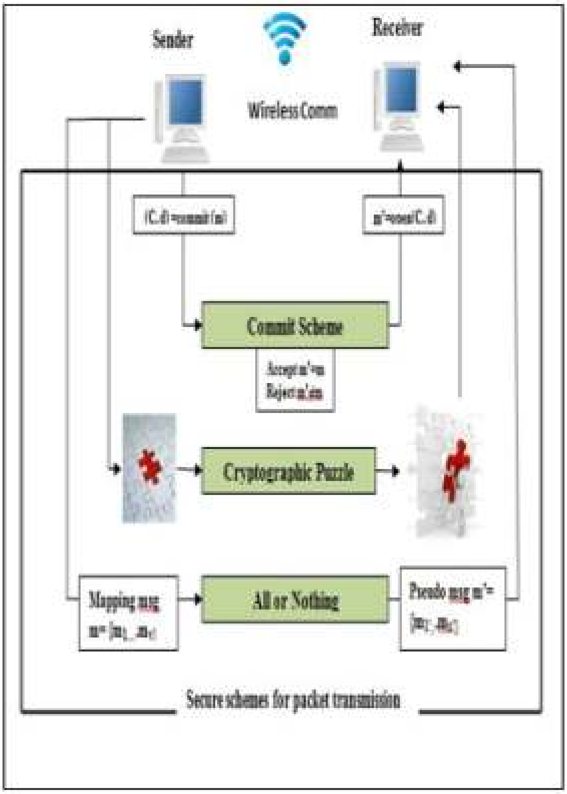

Fig. 3 System Architecture

V. SYSTEM IMPLEMENTATION

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. Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V while keeping m hidden. Commitment schemes are formally defined as follows:

COMMITMENT SCHEME

A commitment scheme is a two phase interactive protocol defined as a triple {X, M, E}. Set X{A,V} denotes two probabilistic polynomial-time interactive parties, where A is known as the committer and V as the verifier; set M denotes the message space, and set E={(ti,fi)}denotes the events occurring at protocol stages ti(i=1.2),as per functions Fi(i=1.2),. During commitment stage t1, A uses a commitment function f1= commit ( ) to generate a pair (C, d)= commit(m), where (C,d) is called the commitment/decommitment pair. At the end of stage t1, A releases the commitment C to V. In the open stage t2, A releases the opening value d. Upon reception of d, V opens the commitment C, by applying function f2 =open ( ), thus obtaining a value of m'= open(C, d). This stage culminates in either acceptance (m'= m) or rejection (m'≠ m) of the commitment by V. Commitment schemes satisfy the following two fundamental properties:

- Hiding. For every polynomial-time party V interacting with A, there is no (probabilistic) polynomially efficient algorithm that would allow V to associate C with m and C' with m', without access to the decommitment values d or d', respectively, and with non-negligible probability.

- Binding. For every polynomial-time party A interacting with V, there is no (probabilistic) 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.

In our context, the role of the committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. The committed value m is the packet that S wants to communicate to R. To transmit m, the sender computes the corresponding commitment /decommitment pair (C, d), and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the decommitment value d, in which case m is obtained by all receivers, including J. Note that the hiding property, as defined in commitment schemes, does not consider the partial release of d and its implications on the partial reveal of m. In fact, a common way of opening commitments is by releasing the committed value itself.

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 predefined 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 puzzle-based scheme is that its security does not rely on the PHY-layer parameters. However, it has higher computation and communication overheads. 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.

Let a sender S have a packet m for transmission. The sender selects a random key k 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. After generating the puzzle P, the sender broadcasts (C,P). At the receiver side, any receiver R solves the received puzzle P' to recover key k' and then computes m' . 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 shows the details of CPHS.

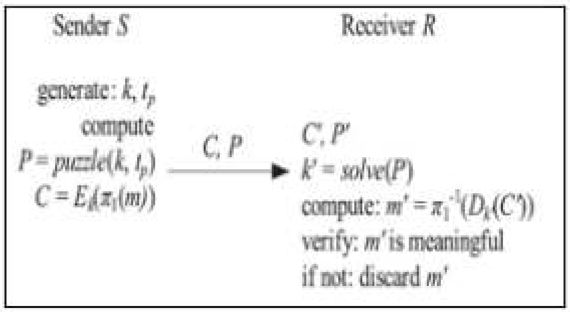

Fig. 4 The cryptographic puzzle based hiding scheme (CPHS)

HIDING BASED ON ALL-OR-NOTHING TRANSFORMATIONS (AONTS)

In this section, we propose a solution based on all-or- Nothing Transformations that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. An AONT serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f, mapping message m = {m1, . . .,mx}to a sequence of pseudo messages m' ={m1' . . .,mx'}, is an AONT if : 1) f is a bijection, 2) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown, and 3) f and its inverse f-1are efficiently computable. When a plaintext is preprocessed by an AONT before encryption, all cipher text blocks must be received to obtain any part of the plaintext. In our context, packets are preprocessed 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. Fig. 5 shows the details of CPHS.

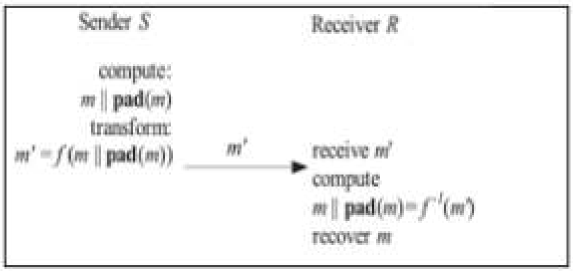

Fig. 5 The AONT based hiding scheme

VI. CONCLUSION

Proposed scheme addressed the problem of selective jamming attacks an internal adversary model in which the jammer is part of the network under attack in wireless networks. The jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. The impact of selective jamming attacks on network protocols such as TCP and routing is evaluated. Our findings show that a selective jammer can significantly impact performance with very low effort. Three schemes that transform a selective jammer to a random one by preventing real-time packet classification are developed and prevent jamming attacks in wireless networks. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with Physical-layer characteristics.

II. FUTURE ENHANCEMENT

The adaptive protocol can be designed to determine the life time of an attacker in the network and the attack pattern can be identified and thus can prevent the network from the denial of service attacks.

VIII. REFERENCES

[1] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[2] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[3] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

[4] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.

[5] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.

[6] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks," Proc. Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.

[7] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," Proc. IEEE NFOCOM, 2010.

[8] R.C. Merkle, "Secure Communications over Insecure Channels," Comm. ACM, vol. 21, no. 4, pp. 294-299, 1978.

[9] C. Po¨pper, M. Strasser, and S. _Capkun, "Jamming-Resistant Broadcast Communication without Shared Keys," Proc. USENIX Security Symp., 2009.

[10] R. Rivest, "All-or-Nothing Encryption and the Package Transform," Proc. Int'l Workshop Fast Software Encryption, pp. 210-218, 1997.

[11] R. Rivest, A. Shamir, and D. Wagner, "Time-Lock Puzzles and Timed-Release Crypto," technical report, Massachusetts Inst. Of Technology, 1996.

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

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

[14] M. Strasser, C. Po¨pper, S. _Capkun, and M. Cagalj, "Jamming- Resistant Key Establishment Using Uncoordinated Frequency Hopping," Proc. IEEE Symp. Security and Privacy, 2008.

[15] 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.

[16] 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.

[17] 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.

[18] 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.