Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 65-68

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Prevent Jamming Attack for Secure Transmission and Packet Hiding

S. Britto Raj A.P and Dr. V. Khana

Dean, Bharath University

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
Jamming attack, SHCS, CPHS

ABSTRACT

In this paper, the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. The adversary exploits his internal knowledge for launching 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. 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.

To Cite This Article: S. Britto Raj A.P and Dr. V. Khana, Prevent Jamming Attack for Secure Transmission and Packet Hiding. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 65-68, 2015*

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 eaves- dropping 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 "al- ways-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 extensively on spread-spectrum 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

Corresponding Author: S. Britto Raj, Dean, Bharath University
E-mail: brittorajs@gmail.com

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.

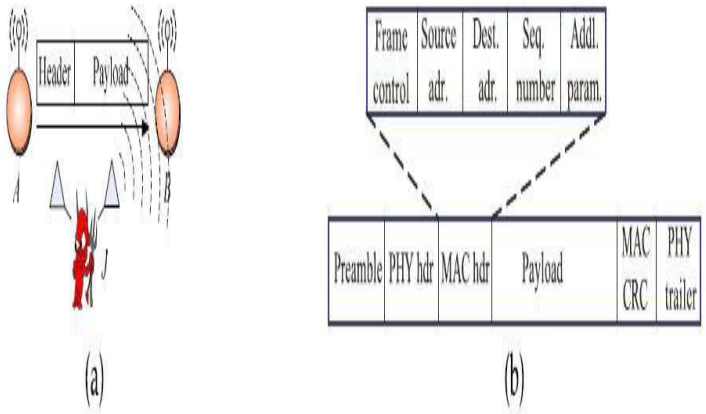

Fig. 1: (a) Realization of a selective jamming attack. (b) A generic frame format for a wireless network.

Existing system:

The existing system address the of problem jamming under an internal adversary model in which the jammer is aware of the implementation details of the network protocols. By utilizing this knowledge, the adversary launches selective jamming attacks in which it targets specific packets of "high" importance. Selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be done by receiving a few bytes of a packet. To launch selective jamming attacks, the jammer must be capable of implementing a "classify then- jam" policy before the completion of a wireless Transmission. Jamming attacks are much harder to counter and have more security problems. They have been shown to cause severe Denial-of-Service (DoS) (Shio Kumar Singh, 2011) attacks against wireless networks. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal. Under this model; jamming methods include the continuous or random transmission of high power interference signals.

Proposed system:

The proposed model we used Strong Hiding Commitment Scheme (SHCS) and Cryptographic Puzzle Hiding Scheme (CPHS) for preventing jamming attacks in networks (Juels, 1999; Rivest, 1996). In Proposed System, 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.

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.

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.

Strong hiding commitment scheme (shcs):

We propose a strong hiding commitment scheme, which is based on symmetric cryptography. Our main motivation is to satisfy the s t r o n g hiding property while keeping the computation and communication overhead to a minimum.

Assume that the sender S has a packet m for R.

First S construct (C,d)=commit(m),

where

$C=Ek(\pi 1(m)),d=k$ (1)

Here the commitment function Ek() is an off-the-shelf symmetric encryption algorithm,π1 is a publicly known permutation and k is a randomly selected key of some desired key length s. The sender broadcasts (C//d), where "//" denotes the concatenation operation. Upon reception of d, any receiver R computes

$m = \pi 1\text{-}1(Dk(C))$, (2)

where π1-1 denotes the inverse permutation of π1. To satisfy the strong hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few PHY-layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

Cryptographic puzzle hiding scheme (cphs):

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.

Let a sender S have a packet m for transmission. The senders select a random key k of 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 i t is directly dependent on the a s sume d computational capability of the a d ve r s a r y, denoted by N a n d me a sur ed in computational operations per second. After generating the puzzle P, t h e sender broadcasts (C,P), where
C=Ek(π1(m)).

At the receiver side, any receiver R solves the received puzzle P1 to recover key k1 and then computes
m1 = π1-1(Dk(C)).

If the decrypted packet m1 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 m1 =m. Else, the receiver discards m1. Fig. 2 show the details of CPHS.

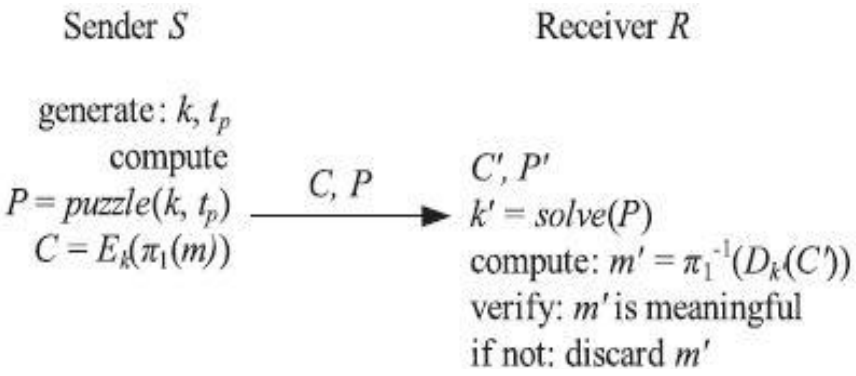

Fig. 2: The cryptographic puzzles-based hiding scheme.

Simulation:

In this module, for each jamming strategy. We observe that a selective jamming attack against RREQ messages is equally effective to a constant jamming attack. However, selective jamming is several orders of magnitude more efficient. On the other hand, random jamming fails to disrupt the route discovery process due to the flooding mechanism of AODV.

Fig. 3: The Sender.

Fig. 4: The Receiver.

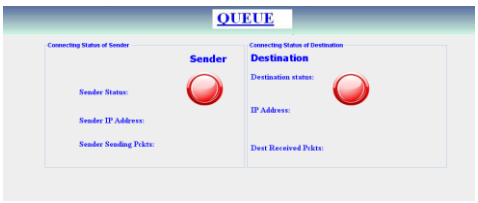

Fig. 5: The Queue.

Fig. 6: Snapshot of NS2 Simulator Outp.

Conclusion:

In this paper the problem of selective jamming attacks in wireless networks has been addressed and 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. Showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing and show that a selective jammer can significantly impact performance with very low effort and developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics and analyzed the security of our schemes and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

REFERENCES

Brown, T.X., J.E. James and A. Sethi, Jamming ans sensing of encrypted wireless ad hoc networks. In proceedings of Mobihoc, pp: 120-130.

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

Lazos, L., S. Liu and M. Krunz, 2009. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pp: 169–180.

Lin, G. and G. Noubir, 2004. On link layer Denial of service in data wireless LANs. Wireless communications and Mobile Computing, 5(3): 273-284.

Oded Goldreich, 2001. Foundations of Cryptography: Volume 1, Basic Tools, (draft available from author's site). Cambridge University Press. ISBN 0-521-79172-3. (See also http://www.wisdom.weizmann.ac.il/~oded/foc-book.html).

Rivest, R., A. Shamir and D. Wagner, 1996. “Time Lock Puzzles and Timed-Release Crypto,” technical report,Massachusetts Inst. of Technology.

Shio Kumar Singh, M., P. Singh and DK. Singh, 2011. “A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks” International Journal of Computer Trends and Technology”Volume 1.

Wilhelm, M., I. Martinovic, J. Schmitt and V. Lenders, 2011. Reactive Jamming in Wireless Networks: How realistic is the threat? In proceddings of Wisec.