ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 182– 186 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Prevent Jamming Attacks in Wireless Networks using Cryptographic Primitives

Kasanavesi.Saketh [#1], Gujula.Neha [*2], Dhanekula Sai Kiran [#3]

[#1] *student , Department of Computer Science and Engineering ,Malla Reddy Institute of Engineering and Technology, Hyderabad .India.*
[*2] *student , Department of Computer Science and Engineering ,Malla Reddy Institute of Engineering and Technology, Hyderabad. India.*
[#3] *student , Department of Computer Science and Engineering ,Malla Reddy Institute of Engineering and Technology, Hyderabad. India.*

[#1] k.saketh123@gmail.com
[*2] gujulaneha26@gmail.com
[#3] saikiranrocks123@gmail.com

ABSTRACT- Jamming is typically referred as an intentional interference attack which is left due to the open nature of u medium. Due to their nature, wireless sensor network are probably the category of wireless networks most vulnerable to radio channel jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of-Service attack on wireless networks. Adversaries with knowledge of protocol specification and network secrets can launch jamming attacks which are difficult to detect. The adversary targets the messages of high priority and huge information when he is active for short period of time. This real time packet classification is done at physical layer. To protect our text from jamming and also to prevent real time packet classification we combine cryptographic primitives with physical layer attributes. There are five schemes for preventing this packet classification. They are Real time packet classification, Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS, All-Or-Nothing Transformation Hiding Schemes (AONTSHS), Channel aware detection algorithm. For providing more secured packet transmission in wireless networks along with the three schemes we use the random key distribution.

Key words–selective jamming, packet classification, denial-of-service, adversaries, primitives, physical layer.

INTRODUCTION

Wireless networks rely on the uninterruptable availability of the wireless medium to interconnect participating nodes. While listening in and message injection can be prevented using cryptographic methods, jamming attacks are much difficult to count. 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. It had been actualized severe denial-of-service(DOS) attacks against wireless networks. In the simplest ways of jamming the adversary interferes with the reception of message by transmitting a continuous jamming signal. Generally jamming attacks have been considered an external threat model in which the jammer is not part of the network .Under this model jamming includes continuous or random transmission of high power interference signals.

Any how while adopting an “all-ways-on” strategy it has several drawbacks. Firstly the adversary has to expand a significant amount of energy to jam frequency bands of interest. Secondly the continuous presence of unusually high interference levels makes this type of attack easy to detect.

The techniques of conventional anti-jamming are extensively on spread spectrum communications. Such as slow frequency hopping or spatial retreats. Spread spectrum techniques provides bit-level protection by spreading bits according to a secret pseudo noise(PN) code known only to the communicating parties under external threat model. These methods only protect wireless transmissions under the internal threat model. Broadcast communications are particularly vulnerable because all of the secrets used to protect transmission. Hence the compromise of a single receivers is sufficient to reveal relevant cryptographic information.

In this paper, we address the problem of jamming under an internal threat model. Now consider a sophisticated adversary aware of network secrets and implementation of network protocols in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. Consider a jammer who 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.

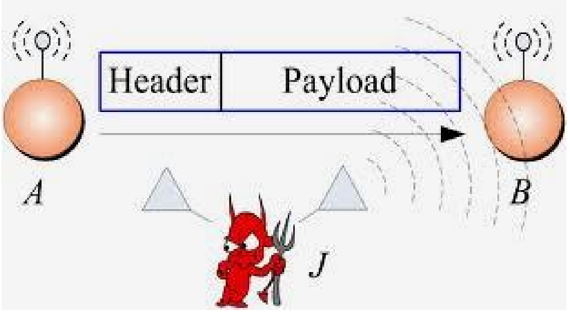

Fig 1: selective jamming attacks for packet classification

EXISTING SYSTEM:

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. Under this model, jamming strategies include the continuous or random transmission of high power interference signals. Conventional anti jamming techniques rely extensively on spread spectrum (SS) communications .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. It can’t prevent node compromise. It can’t prevent selective forwarding attack.

PROPOSED SYSTEM:

In this paper, we address the problem of jamming under an internal threat model. We .Developing a *channel aware detection* algorithm that can effectively identify the selective forwarding attackers by filtering out the normal channel losses. 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 bits 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

ADVERSARY MODEL:

The adversary is in control of the communication medium and can jam messages at any part of the network of his choosing .The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, with the use of multi-radio transceivers. he 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 purpose we assume that the adversary can proactively 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 observed that with far less resources selective jamming can be achieved. A jammer which is equipped with a single half-duplex transceiver is sufficient to jam and classify the transmitted packets. However a model is more effective at high transmission speeds and captures a more potent adversary. The adversary is assumed to be storage boundary, computationally although he can be far superior to normal nodes. In particular for performing any other required computation or any crypt analysis he can be equipped with a special purpose hardware. It is assumed that solving well-known hard cryptographic problems is time consuming. For the purpose of analysis, given a cipher text the corresponding plain text is assumed to be an exhaustive search on the key space. The internal adversary model is realistic for network architectures such as mobile ad hoc, mesh, cognitive radio, and wireless sensor networks, where the devices may operate unattended, thus being susceptible to physical compromise.

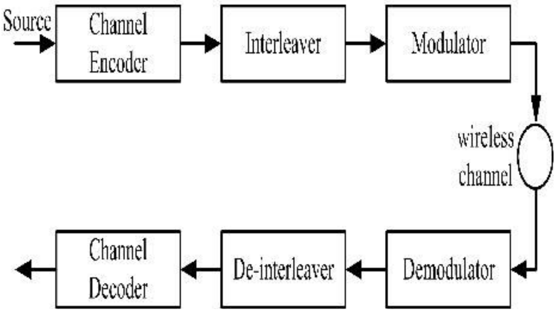

Fig. 2. A generic communication system diagram.

Implementation :

The implementation should be done carefully in order to protect the channel from jamming. If the intruder is having a large knowledge regarding the packet classification. We have to implement the schemes in a proper way. The modules used here are

1) Real Time Packet Classification
2) A Strong Hiding Commitment Scheme
3) Cryptographic Puzzle Hiding Scheme
4) Hiding based on All-Or-Nothing Transformations
5) Channel aware detection algorithm

DESCRIPTION:

Real Time Packet Classification:

Here we are going to describe how the adversary is going to classify the packets in real time, before the packet transmission is done. Once a packet is classified, the adversary may choose to jam it depending on his strategy.

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. The adversary's ability in classifying a packet m depends on the implementation of the blocks. The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors.

A Strong Hiding Commitment Scheme (SHCS):

This scheme is based on symmetric cryptography. Our main aim is to satisfy
the strong hiding property while keeping
the computation and communication overhead
to a minimum. The sender broadcasts (C||d), where "||" denotes the concatenation operation. Upon reception of any receiver. 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):

The main idea behind this scheme is to give the recipient a puzzle and 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. If the recipient is not able to solve the puzzle before the time limit then he is left with nothing.
In this A sender S have a packet m for transmission .The sender selects a random key k , of a desired length. S generates a puzzle (key, time. 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). 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.

Hiding based on All-Or-Nothing Transformations:

The packets are pre-processed by an All-Or-Nothing-Transformations 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.

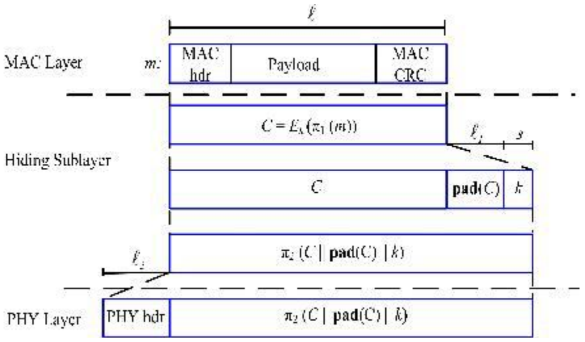

Fig 3: The AONT based hiding scheme

Channel aware detection algorithm:

Selective forwarding attacks are a special case of denial of service (DOS) attack, where a misbehaving mesh router just forwards a subset of the packets it receives but drops the others. It is hard to detect the presence of such attackers because a packet loss over the wireless link can be bad due to the bad channel quality and intentional dropping. In contrast to existing studies, we propose a more practical algorithm known as channel aware detection (CAD) that adopts two strategies, hop-by-hop loss observation and traffic overhearing, to detect the mesh nodes subject to the attack. We derive the optimal detection thresholds by analyzing the false alarm and missed detection probabilities of CAD. We also compare our approach to existing solutions and demonstrate that CAD detects the attackers effectively even in harsh channel conditions.

CONCLUSION:

In this paper the problem of jamming which is most common in wireless networks is been addressed and an internal adversary model in which jammer is a part of the network under attack. We are able to know that the attacker can jam the channel by real time packet classification. This is done by finding the first few symbols of an ongoing transmission. The impact of selective jamming attacks on network protocols such as TCP and routing show that the attacker can make an impact on the performance with a very low effort. Therefore the three schemes mainly commitment schemes, cryptographic puzzles, all-or-nothing schemes prevent the real time packet classification. The channel aware detection algorithm is a special case to prevent this jamming attack. Also the random key distribution is implemented to more secure the packet transmission in wireless networks. Thus by using these schemes the real time packet classification can be stopped and we can protect the radio channel from jamming.

REFERENCES

[1] 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.

[2] R. Rivest, “All-or-Nothing Encryption and the Package Trans- form,” Proc. Int’l Workshop Fast Software Encryption, pp. 210-218,1997.

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

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

[5]. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[6]. A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.

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

[8]. IEEE.IEEE802.11standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[9] 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.

[10] M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti- Jamming Techniques

in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[11] 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.

[12] 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

[13]. 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.

[14]. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.