COMBINING CRYPTOGRAPHIC PRIMITIVES TO PREVENT JAMMING ATTACK IN WIRELESS NETWORKS

HATTARKI.POOJA [1]
Dep. of Computer Science, Appa Institute Of Engineering and Technology Gulbarga, Karnataka,India

ABSTRACT: ***The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of- Service attack on wireless networks. Typically, jamming has been addressed under an external threat model. In this work, we address the problem of jamming attacks and adversary is active for short period of time, selectively targeting the messages of high importance.***
We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All- Or-Nothing Transformation Hiding Schemes (AONTSHS).

Keywords: cryptographic, jamming, Denial-of-Service(DoS)

1. 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) attack 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 highpower 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 thi s 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.

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.

1.1 What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Fig 1.1.1: Diagram clearly explain the about the secure computing

2. LITERATURE SURVEY

2.1 Jamming and Sensing of Encrypted Wireless Ad Hoc Networks

This project considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing. A sensor is developed and tested on live data. The classification is found to be highly reliable for many packet types. The relative roles of size, timing, and sequence are discussed along with the implications for making networks more secure.

2.2 Wormhole-Based Anti-Jamming Techniques in Sensor Networks

AUTHORS: M. Cagalj, S. Capkun, and J.-P. Hubaux

Due to their very nature, wireless sensor networks are probably the category of wireless networks most vulnerable to "radio channel jamming"-based denial-of-service (DoS) attacks. An adversary can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, he prevents them from reporting what they are sensing to the network operator. Therefore, even if an event is sensed by one or several nodes (and the sensor network is otherwise fully connected), the network operator cannot be informed on time. We show how the sensor nodes can exploit channel diversity in order to create wormholes that lead out of the jammed region, through which an alarm can be transmitted to the network operator. We propose three solutions. The first is based on wired pairs of sensors, the second relies on frequency hopping, and the third is based on a novel concept called uncoordinated channel hopping. We develop appropriate mathematical models to study the proposed solutions

2.3 Control Channel Jamming: Resilience and Identification of Traitors

AUTHORS: A. Chan, X. Liu, G. Noubir, and B. Thapa

In this paper, we address the problem of countering jamming of broadcast control channels in wireless communication systems. Targeting control traffic on a system, e.g., BCCH channel in GSM, leads to smart attacks that can be four orders of magnitude more efficient than blind jamming. We propose several schemes based on coding theory and its applications that can counter both external and internal attackers (traitors). We introduce a T-(traitor) resilient scheme that requires less than $(T \log T\ N)^2$ control information transmissions and guarantees delivery of control information against any coalition of T traitors. The proposed scheme also allows the identification of persistently jamming traitors.

2.4 Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study

AUTHORS: T. Dempsey, G. Sahin, Y. Morton, and C. Hopper

Wireless ad hoc networks have fundamentally altered today's battlefield, with applications ranging from unmanned air vehicles to randomly deployed sensor networks. Security and vulnerabilities in wireless ad hoc networks have been considered at different layers, and many attack strategies have been proposed, including denial of service (DoS) through the intelligent jamming of the most critical packet types of flows in a network. This investigates the effectiveness of intelligent jamming in wireless ad hoc networks using the Dynamic Source Routing (DSR) and TCP protocols and introduces an intelligent classifier to facilitate the jamming of such networks. Assuming encrypted packet headers and contents, our classifier is based solely on the observable characteristics of size, inter-arrival timing, and direction and classifies packets with up to "9.4% accuracy in our experiments.

2.5 Improving Wireless Privacy with an Identifier-Free Link Layer Protocol

AUTHORS: B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall

We present the design and evaluation of an 802.11-like wireless link layer protocol that obfuscates all transmitted bits to increase privacy. This includes explicit identifiers such as MAC addresses, the contents of management messages, and other protocol fields that the existing 802.11 protocol relies on to be sent in the clear. By obscuring these fields, we greatly increase the difficulty of identifying or profiling users from their transmissions in ways that are otherwise straightforward. Our design, called SlyFi, is nearly as efficient as existing schemes such as WPA for discovery, link setup, and data delivery despite its heightened protections; transmission requires only symmetric key encryption and reception requires a table lookup followed by symmetric key decryption. Experiments using our implementation on Atheros 802.11 drivers show that SlyFi can discover and associate with networks faster than 802.11 using WPA-PSK. The overhead SlyFi introduces in packet delivery is only slightly higher than that added by WPA-CCMP encryption (10% vs. 3% decrease in throughput).

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

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.

3.2 DISADVANTAGES OF EXISTING SYSTEM:

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.

3.3 PROPOSED SYSTEM:

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.

3.4 ADVANTAGES OF PROPOSED SYSTEM:

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.

4. 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

[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] 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.
[3] 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.
[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.
[5] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.
[6] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009.
[7] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.