SecureMAC: Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks

ABSTRACT

- Wireless network dynamically allocates channel resource to improve spectral efficiency and, to avoid collisions, has its users cooperate with each other using a medium access control (MAC) protocol.
- However, MAC assumes user compliance and can be detrimental when a user misbehaves. An attacker who compromised the network can launch more devastating denial-of-service (DoS) attacks than a network outsider by sending excessive reservation requests to waste bandwidth, by listening to the control messages and conducting power-efficient jamming, by falsifying information to manipulate the network control, and so on.
- We build Secure MAC to defend against such insider threats while retaining the benefits of coordination between the cooperative users. Secure MAC is comprised of four components: channelization to prevent excessive reservations, randomization to thwart reactive targeted jamming, coordination to counter control-message aware jamming and resolve over reserved and under-reserved spectrum, and power attribution to determine each node's contribution to the received power.

CONT….

- Secure MAC is comprised of four components: channelization to prevent excessive reservations, randomization to thwart reactive targeted jamming, coordination to counter control-message aware jamming and resolve over reserved and under-reserved spectrum, and power attribution to determine each node's contribution to the received power.
- Our theoretical analyses and implementation evaluations demonstrate superior performance over previous approaches, which either ignore security issues or give up the benefit of cooperation when under attack by disabling user coordination (such as the Nash equilibrium of continuous wideband transmission). In realistic scenarios, our Secure MAC implementation outperforms such schemes by 76%-159%.

EXISTING SYSTEM

- In wireless MAC security, previous work considers a denialof- service (DoS) attacker capable of either jamming , sending bogus requests to reserve channels, or falsifying information at the communication feedback.
- However, these prior work focus on their respective threats and remain vulnerable when facing a more comprehensive threat model that introduces an attacker capable of performing all of the aforementioned threats.

PROPOSED SYSTEM

- our proposed Secure MAC randomization and coordination, and the centralized scheme that offers fully orthogonal access, either by using no randomization or perfectly orthogonal randomization.
- Because the behavior of each scheme depends on the handshaking list in use, we use three attacker strategies to represent different categories of handshaking list: an attacker that behaves like other legitimate users and contains its transmission within its reserved bandwidth, an attacker that reserves as much spectrum as it can and performs wideband jamming outside that spectrum, since the user uses the ideal handshaking list that excludes the attacker and includes all benign users , *and an* attacker that performs narrowband jamming on the highest priority User.

HARDWARE REQUIREMENTS

- Processor - Pentium-IV
- Speed - 1.1 Ghz
- RAM - 256MB(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Tool - Network Simulator-2
- Operating system - LINUX
- Front end - OTCL (Object Oriented Tool Command Language)

REFERENCES

[1] S.-Y. Chang, Y.-C. Hu, and Z. Liu, “Securing wireless medium access control against insider denial-of-service attackers,” in Proceedings of the IEEE Conference on Communications and Network Security, ser. CNS ’15. IEEE, 2015.

[2] S.-Y. Chang and Y.-C. Hu, “Secure Channel Reservation for Wireless Networks,”.

[3] R. Etkin, A. Parekh, and D. Tse, “Spectrum Sharing for Unlicensed Bands,” vol. 25, no. 3, p. 517, 2007.

[4] J. Chiang and Y. Hu, “Dynamic Jamming Mitigation for Wireless Broadcast Networks,” in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008, pp. 1211–1219.