Secret-Message Transmission by Echoing Encrypted Probes - STEEP

Tech ID: 33702 / UC Case 2024-716-0

CONTACT

Venkata S. Krishnamurty
venkata.krishnamurty@ucr.edu
tel: .

OTHER INFORMATION

KEYWORDS

network security, satellite communications, secret key generation, secret message transmission, secure communication, internet of things, IoT, connected vehicles

CATEGORIZED AS

- **Communications**
  - Internet
  - Networking
  - Wireless
- **Computer**
  - Security
- **Security and Defense**
  - Cyber security

RELATED CASES

2024-716-0

FULL DESCRIPTION

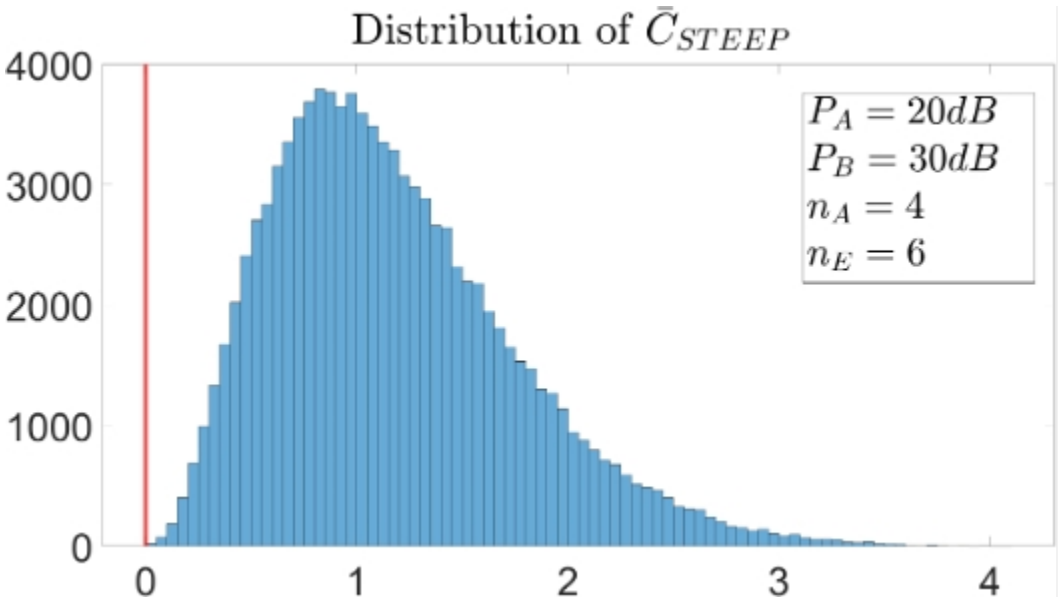
Background

For secure communications between two or more legitimate nodes before there is a shared secret key, the traditional wire tap chanel (WTC) method yields zero secrecy when eavesdropper's channel is stronger than those between the legitimate nodes.

Technology

Prof. Yingbo Hua has developed a round-trip, secure communication scheme - called STEEP, which takes advantage of channel probing for secret-message transmission. The way STEEP works is as follows:

- During phase 1, Alice transmits random probes to Bob. Eve, the eavesdropper also receives these probes but with non-zero noises, which may or may not be larger than the noises at Bob.
- During phase 2, Bob encrypts his estimated probes with a secret message. The encrypted echoes are sent back to Alice over any (public or not) channel. Consequently, Eve cannot decipher the secret message from Bob while Alice can. This is because the virtual (not physical) receive channel at Alice (with the exact knowledge of the probes) is always better than at Eve (with noisy estimates of the probes).



Distribution of the secrecy capacity in bits per probing sample over 100,000 random realizations of all channels between Alice, Bob and Eve, with independent and identically distributed Gaussian elements of unit variance and Gaussian noises with unit variance.

ADVANTAGES

- STEEP enables a quantum leap in physical layer security, i.e., almost always a positive secrecy rate in real-time. This property does not apply to any other physical layer security methods.
- Applicable to various channel types - both analog and digital.
- Complements traditional security methods and can be easily integrated.
- Applicable to various network layers - from the physical layer up to higher layers.
- Efficient in digital implementation as STEEP is a simple round-trip transmission scheme.
- STEEP offers a low-latency and practical approach to secure communication.

SUGGESTED USES

- Scenarios where eavesdropper might have a channel advantage - especially in cases such as satellite communications.
- Multi-hop digital networks such as mesh networks where data traverses multiple nodes before reaching the destination.
- Situations that require frequent refreshing or generation of new secret keys - such as IoT devices and connected vehicles.

INVENTOR INFORMATION

- Please review all inventions by Prof. Hua and his team at UCR.
- Please visit Prof. Hua's website to learn more about his team's research at UCR.
- Please review recent news coverage of Prof. Hua's research at UCR.

RELATED MATERIALS

- Secret-message Transmission by Echoing Encrypted Probes - STEEP
- Unification of Secret Key Generation and Wiretap Channel Transmission
- A Method for Low-Latency Secure Multiple Access

PATENT STATUS

Patent Pending

University of California, Riverside

Office of Technology Commercialization

200 University Office Building,

Riverside,CA 92521

otc@ucr.edu

research.ucr.edu/