THE BUSINESS PARTNER
FOR YOUR IDEAS

SECRET KEY EXCHANGE FOR WIRELESS COMMUNICATIONS

COMPUTING

A new methodology to exchange a random secret key between two parties.

TECHNOLOGY TYPE

Cyber Security
Wireless Communication
Data Transfer
Encryption
Key Generation

IP PROTECTION

U.S. Utility Patent Issued
Method and system for high rate uncorrelated shared secret bit extraction from wireless link characteristics
US8515061B2

Nationalized PCT Issued in United States
Method and system for secret key exchange using wireless link characteristics and random device movement
US8503673B2

LEARN MORE

Reference Number: U-4429

Dean Gallagher
Technology Manager
dean.gallagher@tvc.utah.edu
801-585-0396

TECHNOLOGY SUMMARY

Secret key establishment between two entities is a fundamental requirement for private communication. The most common method for establishing a secret key is by using public key cryptography. The public key method, however, is vulnerable to security breaches, consumes significant amount of computing resources, has been relatively slow, and requires a third party authentication service.

The proposed method represents a fundamental advancement in secret key exchange for wireless communications by avoiding use of a public key. It allows for the exchange of a random secret key between two transceivers by measuring particular bio-directional properties of the channel, which cannot be read at a third location. The properties may include measurements while moving a transceiver to different locations to observe the secret key. The method takes advantage of the changing space-time wireless channel in order to generate a rich and robust key which can be shared on a wireless link without communicating the secret key.

FEATURES AND BENEFITS

- More secure than traditional public key methods.
- No transmission of secret key.
- Secret key can be regenerated at any time.
- Reduces power use and increases key generation rates.

STAGE OF DEVELOPMENT

- Proof of concept established.
- Implemented on android mobile devices.
- Development for other systems and additional functionality still required.

INVENTOR PROFILE

Sneha Kasera, Ph.D., Professor - School of Computing
Neal Patwari, Ph.D., Adjunct Professor - Electrical & Computer Engineering

DATE UPDATED: 7/23/2019