Polarization mode dispersion-based physical layer key generation for optical fiber link security

Tech ID: 29412 / UC Case 2018-533-0

CONTACT

Edward Hsieh
hsiehe5@uci.edu
tel: 949-824-8428.

BRIEF DESCRIPTION

Researchers at UCI have developed a novel method for encrypting optical communications, which is simpler, less expensive, and less computationally-demanding than standard solutions.

SUGGESTED USES

For the encryption of point-to-point optical links

FEATURES/BENEFITS

» Highly random: Encryption is achieved through the polarization mode dispersion (PMD) of a given optical fiber which is highly random (>98%) and therefore impossible to predict.

» Simple, inexpensive: As the encryption method relies on a physical layer inherent within the PPOL system, it offers a low-cost easily-implemented solution.

FULL DESCRIPTION

Recent advancements in the accessibility and bandwidth of optical networks have lead to the rise of optical fiber-based communications, called point-to-point optical links (PPOLs), which are used in applications ranging from ethernet systems to telecommunications and military correspondence. Like any other method of communication, optical fibers are vulnerable to a number of security threats including eavesdropping, message interception, and attacks on the network infrastructure. Though there are a number of methods that can be used to encrypt optical communications, these methods are typically impractical, complicated, time-consuming, and/or computationally demanding. Currently, there is no universal simple, efficient, and safe method for encrypting optical communications. Researchers at UCI have sought to overcome these issues by creating a novel method for PPOL encryption. The encryption here is generated from the dispersion of the polarization modes sustained within an optical fiber as this dispersion is entirely random, unique to the fiber of interest, and impossible for an outsider to predict or determine. This method will be particularly useful for resource-limited applications, where reduced cost and low-power solutions are desired.

STATE OF DEVELOPMENT

Currently in the development stage. PMD-based encryption has been verified; researchers are now working to optimize the key generation algorithm.

PATENT STATUS

Country	Type	Number	Dated	Case

INVENTORS

» Boyraz, Ozdal

» Faruque, Mohammad

OTHER INFORMATION

CATEGORIZED AS

» **Optics and Photonics**
  » All Optics and Photonics
» **Communications**
  » Internet
  » Networking
  » Optical
  » Wireless
» **Computer**
  » Security
» **Security and Defense**

United States Of America	Issued Patent	10,903,992	01/06/2021	2018-533	

» Cyber security
» Other
» **Engineering**
» Other

RELATED CASES

2018-533-0

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- In-Sensor Hardware-Software Co-Design Methodology of the Hall Effect Sensors to Prevent and Contain the EMI Spoofing Attacks
- Tracking Diet And Nutrition with a Wearable Bio-Iot

UCI Beall
Applied Innovation

5270 California Avenue / Irvine,CA
92697-7700 / Tel: 949.824.2683