**AsIOT SECURITY ENHANCEMENT USING PHYSICAL LAYER SIGNATURES**

**Abstract:**

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It provides transparent and seamless incorporation of heterogeneous and different end systems. The connected devices will spread highly sensitive personal data. Sending this type of data represents a serious risk for people’s privacy, since malicious interests could lead to an illegitimate use of personal information. People may hence resist the IOT as long as there is no public confidence that it will not cause any serious threats to their privacy. Effective secure key management for authentication of the devices is the prerequisite of security operations.

A secure wireless communication system involves authentication and secure transmission. Authentication verifies the user identity and prevents malicious users from accessing the network, while secure transmission protects data integrity and confidentiality using encryption schemes. Although the cryptographic schemes such as ECDH have been efficient in protecting modern communication and computer networks, their applications in IoT have been challenged. This is because conventional schemes are based on complex mathematical problems and protocols. These schemes work well for devices having powerful capabilities, such as smartphones. On the other hand, there are a large amount of IoT devices that are of low cost, small size, and battery-powered, such as Fitbit. These lightweight devices may not be able to support computationally complex algorithms needed to perform the complex cryptography.

A new model for security is hence proposed.

* To develop a new secret key generation algorithm using physical layer signatures like CSI
* To overcome key exchange, key distribution and key management
* overhead at legitimate users.
* To provide significant improvement in secrecy.