Poster ID: 10

Hong Zhao, 3rd Year Ph. D Student
The University of Aizu

Poster Session at Graduate School Information Fair

Efficient and Appropriate Key Generation Scheme in Different IoT Scenarios

General Background

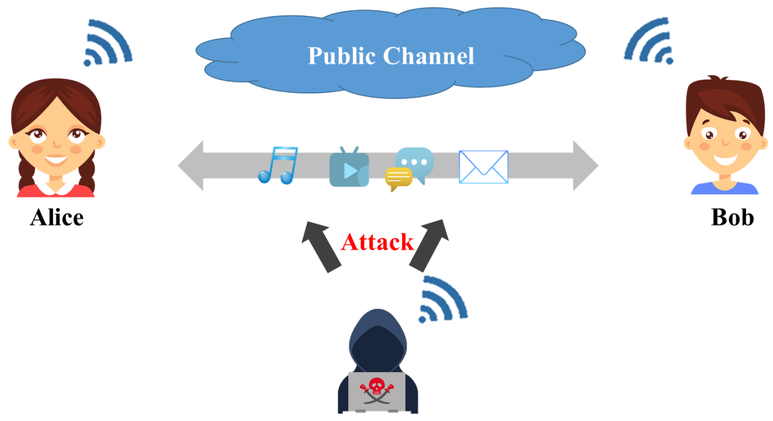

Fig. 1. IoT device communication scenario.

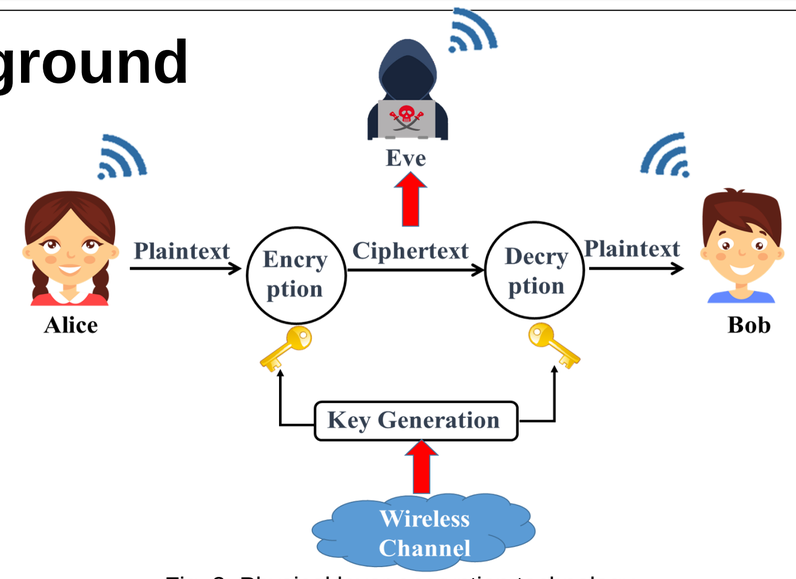

Fig. 2. Physical layer encryption technology.

Problem

- Various threats
- low-power and energy-constrained wireless devices
- Public Channel

Solution

Physical layer encryption utilizing the **unpredictability** and **randomness** of the wireless channel by communication parties.

Advantages

The keys source come from the wireless channel

Do not need to the third-party key distribution center.

Efficient and Appropriate Key Generation Scheme

Research Challenges

The measurements in different scenarios have different features.

- Static scenario: high similarity, lower volatility, lower entropy, and easier mutation
- Dynamic scenario: low reciprocity, high volatility, and high entropy

Due to the characteristics of values, the requirements for key generation performance in different scenarios are also different

My Approaches

From the above analysis, we get the characteristics of the channel values and the requirements for key generation in different scenarios. Additionally, the emphasis on key generation performance varies depending on the scenario. We design the key generation scheme that is appropriate for various scenarios, called EAKGS.

Overview of EAKGS

Channel data collection	Alice keeps sending index probe packets to Bob. When Bob receives the signal, he responds with an acknowledgment signal. Alice and Bob collect data multiple times during coherence time and record the data as *rss_a* and *rss_b*, respectively.
Prejudgment of channel data	We use the variance to pre-judge the channel data. If the variance of the measured data is less than *th*, it is judged to be the measured value of the static scene and run SKGP, otherwise it is the measured value of the dynamic scene, then run DKGP.
Key generation procedure SKGP and DKGP	SKGP and DKGP make up the key generation procedure. The primary objective of this stage is to generate share keys through processes like preprocessing, quantization, privacy amplification, or key reconstruction.
SKGP	• Preprocessing (Amplitude limiting) • Synchronize Quantization • Privacy Amplification
DKGP	• Preprocessing (Discrete cosine transform) • Adaptive Iteration Quantization • Key Reconstruction

Scheme Design and Analysis for EAKGS