# Protecting Secret Key Generation Systems Against Jamming Energy Harvesting and Channel Hopping Approaches

## ABSTRACT

Secret key generation (SKG) from shared randomness at two remote locations has been extensively studied and has recently been extended to unauthenticated channels. SKG techniques have also been incorporated in protocols that are resilient to spoofing, tampering and man-inthe-middle active attacks. Still, such key generation techniques are not entirely robust against active adversaries, particularly during the advantage distillation phase. Denial of service attacks in the form of jamming are a known vulnerability of SKG systems, it was demonstrated that when increasing the jamming power, the reconciliation rate normalized to the rate of the SKG increases sharply and the SKG process can in essence be brought to a halt. As SKG techniques are currently being considered for applications such as the Internet of things.

## EXISTING SYSTEM

In Existing System, two main counter-jamming approaches have been commonly considered: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). In either approach, the impact of power constrained jammers can be limited because their optimal strategy has been proved to be the spreading of their available power over the entire bandwidth (and thus jam with potentially low power). However, DSSS and FHSS systems require a pre-shared secret to establish the spreading sequence or the hopping pattern at Alice and Bob; as such, they are not directly applicable to SKG systems that on the contrary seek to establish a secret key. Attempting to resolve this contradiction and reconcile DSSS and FHSS with SKG, uncoordinated frequency hopping and spreading techniques. The main idea behind the proposed approaches was the randomization of the selection of the hopping/spreading sequences, at the cost of reducing the achievable rates for secret key establishment.

## DIS ADVANTAGES

- It provides lower utility against a spreading jammer.
- Harvesting energy becomes time-consuming and inefficient in terms of SKG capacity.

## PROPOSED SYSTEM

In Proposed System, two counter-jamming approaches are investigated for SKG systems: first, the employment of energy harvesting (EH) at the legitimate nodes to turn part of the jamming power into useful communication power, and, second, the use of channel hopping or power spreading in block fading channels to reduce the impact of jamming. In both cases, the adversarial interaction between the pair of legitimate nodes and the jammer is formulated as a two-player zero-sum game and the Nash and Stackelberg equilibria (NE and SE) are characterized analytically and in closed form.

## ADVANTAGES

- It does not leak any information to eavesdroppers.
- SKG process can be made error free.

## SYSTEM REQUIREMENTS

**H/W System Configuration:-**

| | | |
|---|---|---|
| Processor | - | Pentium –III |
| RAM | - | 256 MB (min) |
| Hard Disk | - | 20 GB |
| Key Board | - | Standard Windows Keyboard |
| Mouse | - | Two or Three Button Mouse |
| Monitor | - | SVGA |

**S/W System Configuration:-**

| | | |
|---|---|---|
| Operating System | : | Windows95/98/2000/XP |
| Application Server | : | Tomcat5.0/6.X |
| Front End | : | HTML, Jsp |

| | | |
|---|---|---|
| Scripts | : | JavaScript. |
| Server side Script | : | Java Server Pages. |
| Database | : | MySQL 5.0 |
| Database Connectivity | : | JDBC |