Novel Secret Key Generation Techniques with Application in Cognitive Radio Networks

Ahmed Badawy, PhD Student, 29th Cycle, Year II, ID: 35049

Supervisors: Dr. Daniele Trinchero and Dr. Carla-Fabiana Chiasserini

Collaborators: Dr. Tamer Khattab, Dr. Tarek Elfouly, and Dr. Amr Mohamed from Qatar University
Outline

- List of attended classes
- Research context and motivation
- Addressed research problems
- Novel contributions
- Adopted methodologies
- List of submitted and published conference/journal papers
- Future work
List of Attended Classes

- Hard Skill Courses
  - Radio Planning (01NQUOT):
    8 Credits – Pass with merit – awarded points: 66.67
  - Innovative wireless platforms for the internet of things (01OVEPE):
    6 Credits - Pass with merit – awarded points: 50
  - Embedded electromagnetic for the internet of things (01QFARN):
    4 Credits – Grade not given yet.

- Soft Skill Courses
  - Attending two courses at Qatar University
    • Applied Research Methodology: 42 hours
    • Graduate Research Seminar: 42 hours
Research Context

- Conventional Cryptographic techniques mandate the exchange of encryption keys at one point during the encryption--decryption process.
- This poses a serious threat to the secrecy of the whole communication session.
- Another main drawback is the necessity of a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers.
- Physical layer security relies on randomness characteristics inherent in the communication channels, which are common to the two trusted parties, which being unknown to a potential eavesdropper.
- Thus, key exchange is no longer mandatory and key renewal is potentially possible for every packet transmission.
Research Context

- This results in a higher secrecy potential than upper layers cryptographic methods while maintaining lower computational complexity.
- Within the paradigm of physical layer security, a physical layer characteristic is used as a common source of randomness to generate the secret key.
- In cognitive radio networks, secondary users (SUs) communicate on unused spectrum slots in the frequency bands assigned to primary users (PUs).
- Two of the major physical layer attacks against cognitive radio networks are spectrum sensing data falsification (SSDF) and eavesdropping.
Motivation

- Secret key generation based on channel estimates has several drawbacks that include predicting the channel by an attacker who employs ray-tracing algorithm, rectangular room problem as well as channel being static.
- Secret key generation based on distance is susceptible to recovered if the eavesdropped is equipped with angle of arrival estimation capabilities.
- The former drawbacks urges the need for developing a secret key generation technique that can overcomes these downsides.
- A main drawback in almost all of the existing physical layer security techniques, whether it is based on channel gain, RSS or distance, is their poor performance at low signal to noise ratio (SNR).
- The former drawback urges the need for a secret key generation techniques that can operate sufficiently at low SNR levels.
- Due to the nature of cognitive radio networks, conventional physical layer security schemes are not typically used.
- This urges the need to developing physical layer security schemes that suit the nature of the cognitive radio network.
Addressed Research Problems

- Drawbacks of current state-of-the-art secret key generation methods
- Novel physical layer characteristic that can be used at low SNR conditions
- Physical layer security techniques that adapt to the nature of cognitive radio networks.
Novel Contribution

- **Drawbacks of conventional physical layer security methods**
  - It was noted that some common sources of randomness are estimated simultaneously such as channel gain and phase, and RSS and distance.
  - Combining multiple common sources of randomness can drastically improve the performance of secret key generation. We combined channel and distance measurement to improve the performance of secret key generation.

- **Novel Physical layer security schemes**
  - It was noted that angle of arrival (AoA) between the two legitimate nodes if measured from a common reference can be considered common.
  - It was noted that AoA can be estimated with very high accuracy at very low SNR levels. We developed an algorithm to extract secret key from AoA.
  - Another novel physical layer characteristic is a secondary random process (SRP) that exploits the channel gain or phase to generate a secret key.
  - Both novel physical layer characteristics enhanced the performance of security by improving the bit mismatch rate (BMR).

- **Physical layer security in cognitive radio networks**
  - Exploited the spectrum sensing data as a common sources of randomness to generate secret key.
Novel Contribution

- Secret Key generation based on channel and distance:
  - Achieves lower BMR than channel gain only and distance only.
  - Achieved higher entropy than than channel gain only and distance only.
  - Overcomes the drawbacks of than channel gain only and distance only.
Novel Contribution

- Secret key generation based on AoA estimation:
  - Simulated root mean square error (RMSE) of two AoA estimation algorithms (MUSIC and XSBS), which showed a very small error at very low SNR level.
  - Combined both azimuth and elevation angles, which adds an extra degree of freedom and improves the BMR as well as the entropy.
Novel Contribution

- Secret key generation based on channel secondary random process

Flow chart of secondary random process creation

- Start
- Estimate the threshold $\gamma^t$
- Initialize vector $S_0^t$ to all zeros
- $i = 1$
- If $|H_{0}[i]| > \gamma^t$, then Yes, $S_0^t[i] = i$ and Increment $i$; No, go to $J^t = S_0^t[1:end] - S_0^t[1:end-1]$
- If $i \leq N$, then Yes, go to $J^t = S_0^t[2:end] - S_0^t[1:end-1]$
- No, End

Example of secondary random process of based on channel gain

BMR

Entropy
Novel Contribution

- Secret key generation by exploiting the spectrum sensing data for cognitive radio networks.

Decision statistic as a common source of randomness at the two legitimate SUs as well as the malicious node.

Shuffled seed used to extract the secret key at the two legitimate SUs.
Adopted Methodologies

- **Surveyed** the current state-of-the-art secret key generation techniques.
- **Defined** a system model for the research problem of generating a secret key based on novel physical layer characteristics.
- **Collected** initial measurements using FPGA-based WARP Kits for the channel gain and phase of an indoor-lab environment.
- **Conducted** simulation of exploiting novel physical layer characteristics such as angle of arrival, combined channel gain and phase.
- **Developed** an algorithm that exploits AoA to generate secret Key.
- **Developed** an algorithm that creates a channel secondary random processes, which is then used to generate the secret key.
List of submitted/accepted paper

**Accepted Journal Papers:**

**Published Conference Papers:**

**Submitted Conference Paper:**

**Submitted Journal Papers:**
Future Work

- Different hybridization (i.e., combining) functions can be applied on the multiple common sources of randomness with the objective of minimizing the BMR and maximizing the key entropy.
- Find a way to converge the two worlds (physical layer secrecy and cryptographic secrecy) in order to allow for practical comparisons between conventional cryptographic methods and relatively recent physical layer secrecy based methods.
- Conducting performance analysis of secrecy capacity for our secondary random process.
- Exploring new methods for physical layer security adaptable to cognitive radio networks.