Physical-Layer Key Generation for Automotive Cyber-Physical System Security

Jiang Wan, M.S., Anthony Lopez, B.S., Mohammad Al Faruque, Ph.D.
Electrical Engineering and Computer Science
University of California, Irvine

Introduction

- Automotive systems are **computerized**. Over **80 Electrical Control Units** [1].
- **Vehicular communication (V2X)** is a proposed solution to human-caused collisions (80% of all collisions) [2].
- Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) Communication **confidentiality, integrity, and authentication** [1][3].
- **Vehicular wireless channel randomness** is a novel source to quickly generate secret keys with lower storage and energy overhead [4][5].

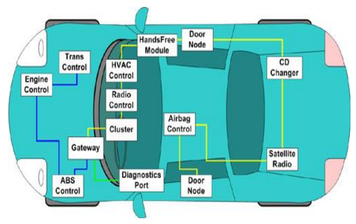


Figure 1. Typical network on vehicle

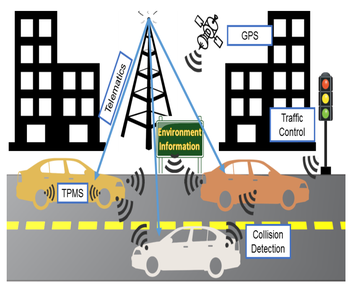


Figure 2. Examples of V2V and V2I Communication

Experimentation with RC Cars

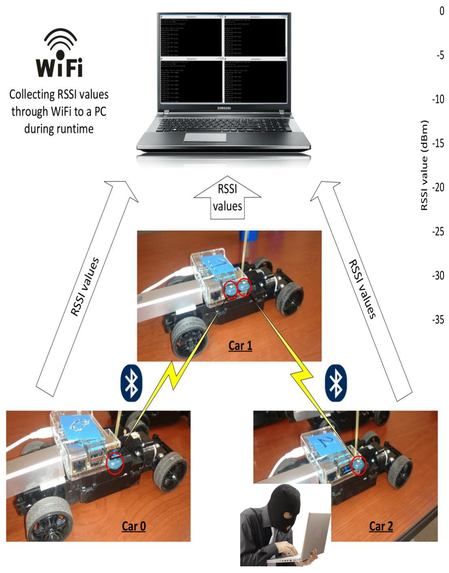
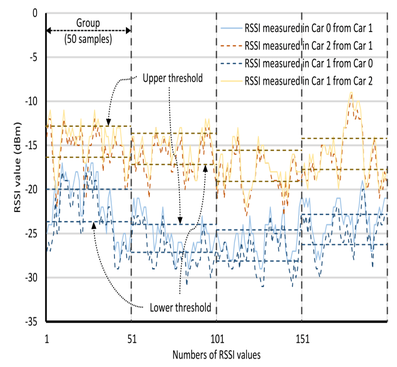


Figure 4. Fetching RSSI Values using PUTTY and simple Bash script to generate keys



	Generated 64-bit Keys
Car 1 from Car 0	1100000110000000_0000000100000110_0000000010000000_0000011111111111
Car 0 from Car 1	1100000110000000_0000000100000110_0000000010000000_0000011111111111
Car 1 from Car 2	0000001111111111_1111000000000000_0000011111100000_0000011110000011
Car 2 from Car 1	0000001111111111_1111000000000000_0000011111100000_0000011110000011

Figure 5. Sample RSSI values and generated secret keys (must be unique)

Summary

- Developed a **fast and novel secret key generation technique** for automotive systems based on RSSI values of wireless channel physical layer.
- Performed proof of concept through experimentation with **RC cars and automobiles**.
- Can **help realize encryption** for vehicular wireless communication security.

Future Work

- **Implement** the algorithm on actual vehicular communication devices and experiment in real-time.
- **Develop new** key generation algorithms dependent on signal phase and channel impulse response.
- **Evaluate** which among these algorithms are fastest, efficient, and secure for automotive networks.

Key Generation

- **Key Bit Quantization Method:**
  If $\mathbf{RSSI_{Value} > Thresh_{Upper}}$ **-> 1**
  If $\mathbf{RSSI_{Value} < Thresh_{Lower}}$ **-> 0**
  Else **keep repeating on rest of values**
- **Wait Time Interval (τ_{step}) >= Coherence Time (T_c)**
- T_c depends on the **absolute velocity difference (ΔV)**
- Mismatching **key bit elimination**

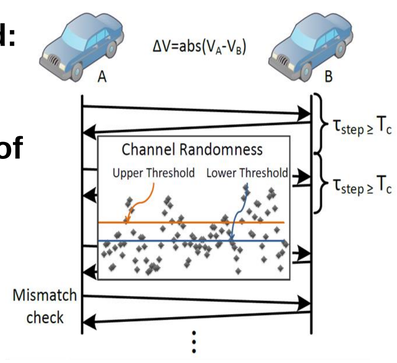


Figure 3. Key Generation Overview

Experimentation with Automobiles

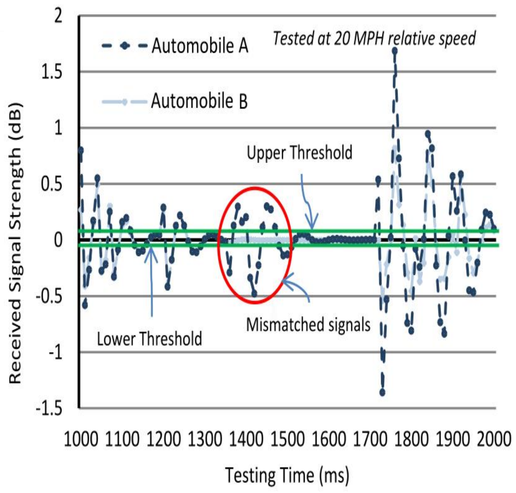


Figure 6 Sample RSSI values and corresponding thresholds

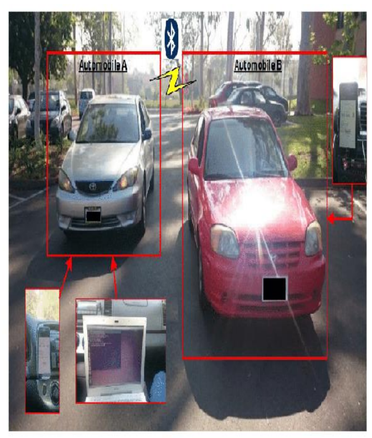


Figure 7 Setup with two automobiles and phones

Attack Model

- **Understands protocol** and can **read messages** over the air.
- **Physically nearby** the targeted vehicles.
- We want to **prevent the attacker from computing the secret key.**

References

1. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., “Comprehensive experimental analyses of automotive attack surfaces,” USENIX Security Symposium, 2011.
2. Weiß. V2x communication in europe–from research projects towards standardization and field testing of vehicle communication technology. Computer Networks, 55(14):3103–3119, 2011.
3. T. Schutze. Automotive security: Cryptography for car2x communication. In Embedded World Conference. Citeseer, 2011.
4. M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. IEEE Transactions on Information Theory, pages 2515–2534, 2008.
5. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radiotelepathy: extracting a secret key from an unauthenticated wireless channel,” Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 128–139, 2008

UC IRVINE