Poster: Physical Layer Key Generation Protocol for Secure V2X Communication Architecture

Kelvin Phan, Arnav Malawade, Anthony Lopez, Anomadarshi Barua,
Preston Rogers, Ken Tran, and Mohammad Al Faruque
University of California Irvine
Email: {kelvinhp, malawada, anthl10, anomadab, parogers, kenct, alfaruqu}@uci.edu

***Abstract*—Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication are part of a growing market of potential solutions to challenges in collision avoidance, traffic control, and environmental hazard detection. Wireless technologies such as Dedicated Short-Range Communications (DSRC) form the basis of this new V2V/V2I communication and are inherently insecure. Safety-related applications such as collision detection also pose time constraints as related communications must be completed within a small time frame. As such, any Vehicle to Everything (V2X) communication protocol should be designed to ensure that communications are secure and, when necessary, can be completed within time constraints. To address these issues, we have developed a wireless communication security protocol designed for time efficiency, low overhead, and reliability in highly dynamic environments like those in which V2X communications are conducted. It employs a physical layer key generator and key length optimization algorithm, utilizing attributes unique to each wireless connection to generate secure keys and optimizing key length to meet real-time requirements as determined by environmental conditions. The technology presented is the work of Mohammad Al Faruque, Jiang Wan, and Anthony Lopez and is patented under patent #15/439,102.**

I. Introduction

A. Motivation

In recent years, connected vehicle technology using Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications has gained market momentum because of interest from both government and industry. In 2016, The National Highway Traffic Safety Administration proposed a mandate that would have required all automakers in the United States to install V2V capability by 2020. Although the proposed rule has not been instated, well-known automakers Toyota and Volkswagen have declared their intent to deploy V2V/V2I technology in the meanwhile [1]. It is predicted that, should the proposed mandate go into effect, there is potential for 60% of vehicles to be equipped with V2V technology by 2029; this is equivalent to 146 million cumulative cars [2]. In the likely scenario that these Vehicle to Everything (V2X) technologies are standard features on autonomous vehicles, the growth of the autonomous vehicle industry bolsters the market for this technology as autonomous vehicles may make up 40% of vehicle travel by the 2040's [3]. Given both government and industry interest in such technology, it can be reasonably concluded that this movement towards connected vehicles will be accompanied by a need for secure wireless communications.

B. Contributions

Current state-of-the-art options for securing wireless communications fall under the following types of encryption algorithms: symmetric, asymmetric, and hybrid. Symmetric algorithms are preferred due to their fast performance but require pre-shared keys, which can be predictable and less secure if standardized keys are used. Asymmetric algorithms allow for randomly generated keys to be exchanged but have slow performance. Since V2X networks often handle safety-critical messages with very strict latency requirements, this rules out asymmetric and hybrid encryption schemes for all but low priority, non-critical messages. From these limitations, it was concluded that secure wireless communication poses the following challenges: **finding a reliable high entropy source to generate secret keys for symmetric key algorithms, designing a reliable solution for management of symmetric secret keys, and optimizing the solution and key size** [4]. Our physical layer key generator and key length optimization algorithm were developed in part to meet these specific challenges, thereby providing a secure wireless communication solution without the limitations of other state-of-the-art options. Our technology provides confidentiality and ensures that wireless communications are kept private from potential attackers since they cannot mimic the physical randomness of the wireless channel between any two given vehicles. Additionally, our technology functions in real-time and is able to provide encryption that meets critical-message latency requirements. An overview of the described physical layer key generation security protocol is shown in Figure 1.

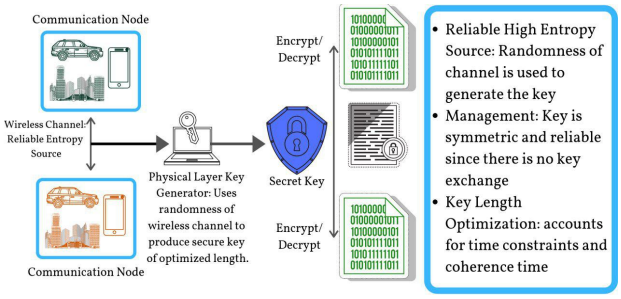


Fig. 1. Key Generation Methodology

This material is based upon work partially supported by the Proof of Product (PoP) Grant from University of California, Irvine Applied Innovation.

II. Problem Statement

A. Objectives

The objective of this project is to create a proof-of-concept prototype which demonstrates that our physical layer key generator can operate reliably in a real-time system and meet industry latency requirements for V2X communication. As such, the criteria of a successful protocol include low latency performance, real-time operation in dynamic environments of varying relative velocities, and the security of data against real-world attack models. The completed device will prove that the communication protocol outlined can be used as a viable data security option for V2X communication.

B. Constraints

Since V2X technology has significant implications for vehicle safety, certain messages such as collision warnings, pre-crash sensing, and emergency braking alerts must have very low latency. This requirement is unique to safety-critical systems and is challenging to meet because the encryption process can introduce significant latency. According to [4], these high-priority messages must have a latency of no more than 200 milliseconds in order to be effective at preventing crashes.

III. Technical Approach

A. IEEE 802.11p

Previous related work in [4] demonstrated real-world experiments using Bluetooth radios to communicate between nodes. The de facto standard for V2X communication is IEEE 802.11p, which is an amendment to IEEE 802.11 that operates on the 5.9 GHz frequency band and is adapted for the requirements of vehicular networks. [5] developed a Wireless LAN (WLAN) transceiver in GNURadio as part of the contributions of his research. In the interest of better emulating real-world operation, we use the Software Defined Radio (SDR)-based WLAN transceiver from [5] on Ettus B210 boards, shown in Figure 2, in our experimental setup. Currently, each "vehicle" is emulated using a personal computer (PC) and a connected Ettus B210; GNU Radio is used to program and control the B210s from the PCs. This establishes a wireless communication channel between the two systems from which relevant channel data can be extracted.

Fig. 2. Ettus B210 Software Defined Radios

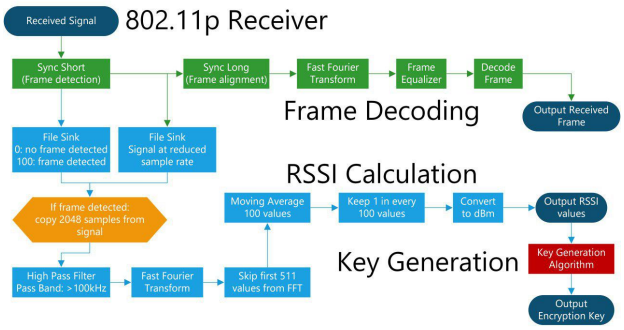


Fig. 3. RSSI Sequence Extraction: RSSI sequence is calculated when an 802.11p frame is detected.

B. RSSI Sequence Extraction

Given that there is no existing API to calculate Received Signal Strength Indicator (RSSI) values for the B210, we leverage a GNU Radio SDR implementation for RSSI calculation from [6]. Upon frame detection, raw samples for the given frame are streamed to a file and retrieved by our RSSI calculation algorithm. The RSSI algorithm creates a sequence of RSSI values for the frame which are then used as a seed sequence for our key generator. Figure 3 describes the purpose of each module within the RSSI calculation module in greater detail.

C. Key Generation

The key generation algorithms used for our project are from [4] as they have been demonstrated to work on RSSI values in the past. We will be adapting the algorithms for higher accuracy in industry-standard 802.11p channels.

IV. Conclusion

Overall, we have developed a proof-of-concept prototype to demonstrate that our physical layer key generator, which is based on the unique channel between two nodes, can operate reliably in a real-time system and meet critical message latency requirements using industry standard protocols. Continuing this work, we will be augmenting our algorithm with the ability to optimize key length to account for slow or fast fading channels as well as other environmental effects.

References

[1] S. Abuelsamid, "Toyota Has Big Plans To Get Cars Talking To Each Other And Infrastructure In The U.S.," *Forbes*. [Online]. Available: https://www.forbes.com/sites/samabuelsamid/2018/04/16/toyota-launches-aggressive-v2x-communications-roll-out-from-2021/. [Accessed: 02-Aug-2018].

[2] S. Bayless et al., The Impact of a Vehicle-to-Vehicle Communications Rulemaking on Growth in the DSRC Automotive Aftermarket: a Market Adoption Model and Forecast for Dedicated Short Range Communications (DSRC) for Light and Heavy Vehicle Categories, Oct. 2016.

[3] T. Litman, Implications for Transport Planning, p. 39.

[4] J. Wan, A. Lopez, and M. A. A. Faruque, Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems, *Phys. Syst.*, vol. 1, no. 1, p. 28.

[5] B. Bloessl, A Physical Layer Experimentation Framework for Automotive WLAN, p. 157.

[6] T. Mukherjee et al., RSSI-Based Supervised Learning for Uncooperative Direction-Finding, in Machine Learning and Knowledge Discovery in Databases, 2017, pp. 216227.

Physical Layer Key Generation Protocol for Secure V2X Communication Architecture

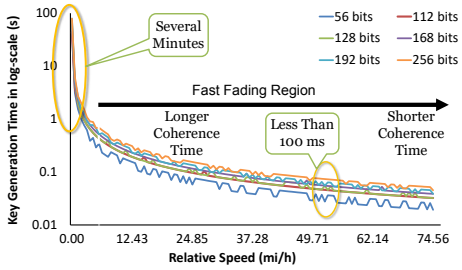
Kelvin Phan, Arnav Malawade, Anthony Lopez, Anomadarshi Barua,
Ken Tran, Preston Rogers, Mohammad Al Faruque
Electrical Engineering and Computer Science
University of California, Irvine

Problem

- Attackers can use insecure V2X networks to send false alerts and steal confidential user data
- Strict latency requirements for safety-critical messages (<200ms)
- Asymmetric/hybrid key encryption schemes are too slow to meet latency requirements
- Symmetric key schemes are fast but cause key management issues and can be deterministic

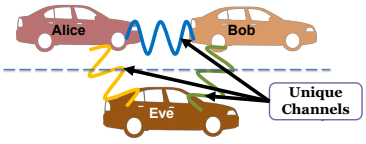
Channel Coherence

Greater relative speed → Channel changes faster



Attack Model

- Eve is non-intrusive eavesdropper who wants to derive the shared key between Alice and Bob
- **Eve will not be able to derive same key** if more than a few wavelengths away from Alice and Bob's channel
- Their key is correlated with their shared channel and not Eve's channel



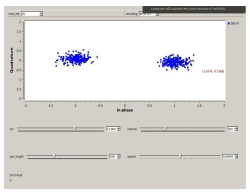
Testbed

Tools Used:

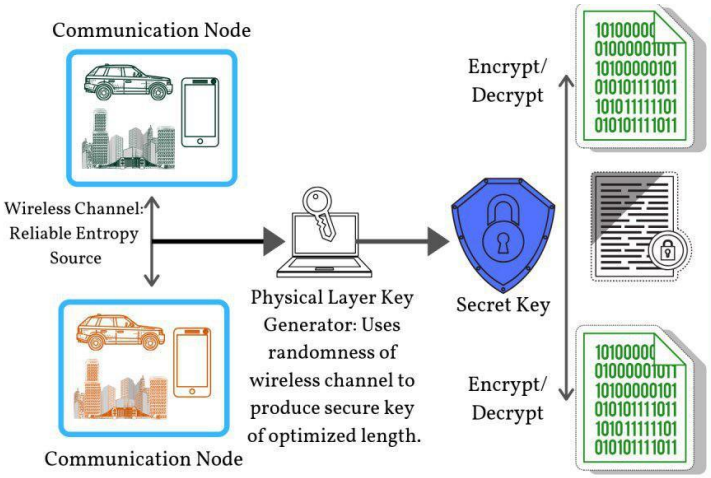
- USRP B210 Software Defined Radio
- GNU Radio SDR Software (Python & C++)
- 802.11p transceiver implemented in GNURadio [1]

Implements industry standard V2X communication protocol 802.11p (5.9GHz)

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM



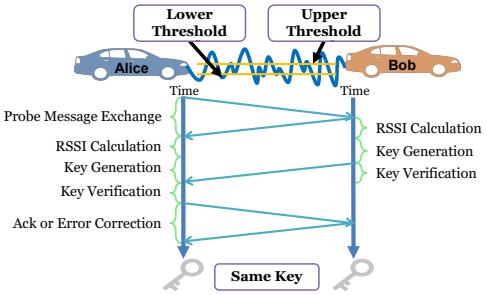
Methodology



- Reliable High Entropy Source: Randomness of channel is used to generate the key
- Management: Key is symmetric and reliable since there is no key exchange
- Key Length Optimization: accounts for time constraints and coherence time

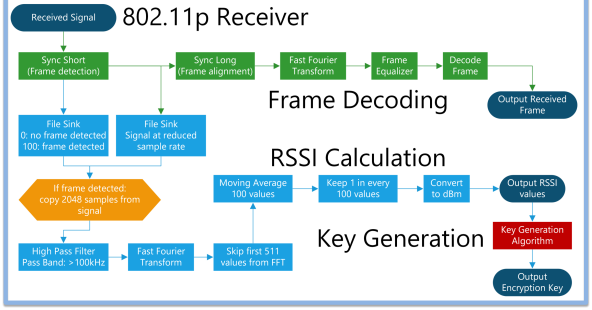
Key Generation

- Vehicles send start message to one another
- Relative Signal Strength (RSSI) calculated over all samples in received start message
- Sequence of RSSI values used to generate unique symmetric encryption key in real time
- lower and upper threshold to map values to "0"s and "1"s
- **Unique channel between the two vehicles → Both vehicles generate same key**
- **Symmetric key encryption used for future messages between the two vehicles → Fast**



Frame-Triggered RSSI Calculation

- RSSI calculation begins when an 802.11p frame is detected
- RSSI values are calculated over the length of the frame
- Sequence of RSSI values used to generate encryption key



Summary

- A proof-of-concept prototype which demonstrates that our **physical layer key generator based on the unique channel between two nodes** can operate reliably in a **real-time** system and meet **critical message latency requirements** using **industry standard protocols.**
- Our algorithm will optimize key length to account for slow or fast fading channels and other environmental effects

Future Work

Dynamic Testing and Optimization

- Test real-time performance of algorithm in vehicles at different speeds (fast fading and slow fading channels)
- Test effects of reflection, multi-pathing, absorption, collisions, etc. on channel coherence and algorithm reliability
- Test against real-world attack scenarios
- Optimize key length based on channel coherence and message priority

References

1. B. Bloessl, "A Physical Layer Experimentation Framework for Automotive WLAN", Ph.D, Paderborn University, 2018.
2. J. Wan, A. Lopez, and M. A. A. Faruque, Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems, Phys. Syst., vol. 1, no. 1.

This material is based upon work partially supported by the Proof of Product (PoP) Grant from University of California, Irvine Applied Innovation.