In-Progress: Exploring Tire Pressure Monitoring Systems (TPMS) for Secure Key Generation for Intra-Vehicular Device Authentication

Omar Achkar*, Shahryar Raza*, James McAvoy*, Rushikesh Shirsat†, Neil Klingensmith† and Kyu In Lee*
*Department of Information Science Technology, University of Houston, Houston, Texas 77204
†Department of Computer Science, Loyola University Chicago, Chicago, Illinois 60660
Email: *{oachkar, saraza3, jpmcavoy, klee48}@cougarnet.uh.edu, †{rshirsat, nklingensmith}@luc.edu

***Abstract*—Modern vehicular systems increasingly rely on secure wireless communications for both inter-vehicle and intra-vehicle device interactions. While traditional wireless authentication methods require manual user intervention and complex authentication procedures, zero-interaction authentication has emerged as a promising alternative, leveraging environmental randomness to generate identical keys that are naturally shared between co-located devices. In this work, we explore the potential of using Tire Pressure Monitoring System (TPMS) transmissions as a novel source of environmental randomness for automotive authentication. Through extensive experimentation, we demonstrate that underlying RF signal characteristics of TPMS provide reliable entropy that can be consistently measured by devices within the vehicle while being difficult to be captured from outside. Our evaluation shows 95% bit agreement rate between legitimate in-vehicle devices while external adversarial devices only achieve 50% agreement rate. Such results suggest that TPMS-based authentication could offer a practical, secure, and user-friendly solution for modern vehicular security challenges.**

***Index Terms*—Tire pressure monitoring system (TPMS), Zero-interaction authentication, Device authentication**

I. Introduction

Modern vehicles have evolved far beyond their traditional roles, now functioning as sophisticated mobile computing platforms that continuously exchange data with smartphones, other vehicles, infotainment systems, and fleet management networks. Not only has this increased connectivity improved the user experience and functionality, it also introduces complex security challenges around securing device communications and ensuring proper authentication. For example, traditional methods that depend on pre-shared keys or PINs (used for WiFi and Bluetooth) have become inadequate, especially in the expanding shared mobility market. Unlike personal vehicles that require only occasional device authentication, shared vehicles must support multiple users and devices, creating unique security demands without sacrificing user experience. This calls for lightweight device authentication solutions that not only offer seamless usability, but also provide robust security during frequent device connections and disconnections.

Zero-interaction authentication (ZIA) has emerged as a promising solution to this challenge by leveraging environmental signals to generate shared encryption keys between nearby devices, allowing automatic authentication without requiring any manual input from users. Devices that detect the same

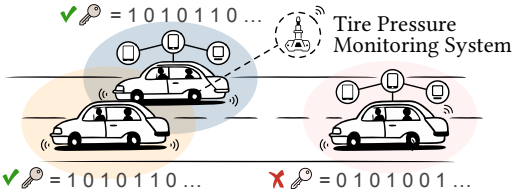

Fig. 1. Vehicle TPMS transmissions create a region of unique signals

environmental randomness, sourced from vibrations [1], [2], ambient audio [3], or motion patterns [4], can independently generate an identical key to authenticate themselves. The success of ZIA depends on consistently capturing high-quality randomness that remains unpredictable to adversaries. However, in dynamic automotive environments, traditional methods often struggle, as varying road conditions and acoustic interference can degrade signal quality and reduce the necessary entropy for secure key generation.

In this work, we introduce a novel approach that leverages the Tire Pressure Monitoring System (TPMS), a mandatory safety feature in all U.S. vehicles, as the basis for secure zero-interaction authentication [5]. Although TPMS transmissions are primarily designed for safety monitoring, their unique signal characteristics, usually broadcasted over RF channels at 315 MHz or 433 MHz, can be used to generate high-entropy random keys. As illustrated in Fig. 1, TPMS signals naturally create a secure authentication zone within the vehicle. Devices located inside this zone receive correlated signals and are able to independently generate identical shared keys, whereas signals captured outside the boundary generate different keys, preventing adversaries from authenticating to legitimate ones. Our initial experimental evaluation, conducted with commodity Software Defined Radio (SDR) hardware in real-world driving conditions, demonstrates that this TPMS-based approach enables legitimate devices to generate keys with 95% agreement rate, while devices outside the vehicle achieve only 50% bit agreement, equivalent to random guessing. This approach offers a promising foundation for lightweight, secure and practical automotive device authentication method.

II. Implementation and Evaluation

Our initial experimentation focuses on validating TPMS signals as a viable source for random, reliable, and correlated

2025 IEEE Security and Privacy Workshops (SPW) | 979-8-3315-6643-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/SPW67851.2025.00050

DOI 10.1109/SPW67851.2025.00050

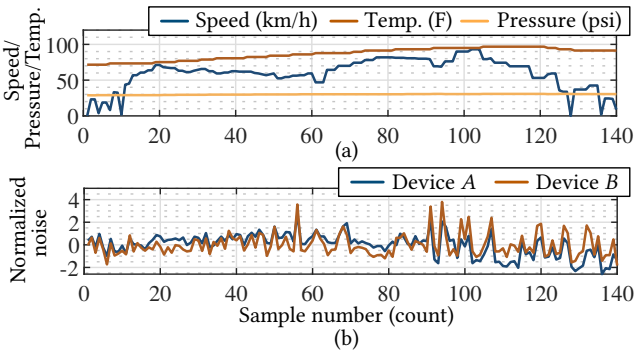

Fig. 2. (a) Speed, temperature, and pressure decoded from single TPMS sensor over 30-minute drive in highway. (b) Noise captured by two devices within the same vehicle.

key generation. Using a 2017 Toyota RAV4 as our baseline vehicle, we position two RTL-SDR V4 receivers (each representing user-owned devices) in the front seats of the vehicle to capture TPMS transmissions from the driver-side front wheel sensor broadcasting at 315 MHz. The two SDRs are then connected to a Linux-based laptop running RTL-433 software [6] for real-time signal decoding and analysis. To further allow more comprehensive analysis of vehicle dynamics, we connect the vehicle's OBD-II port to our laptop using an ELM327 interface, providing access to real-time vehicle speed and other telemetry data. Each time we detect TPMS signal being emitted (about once a minute for each wheel), we record the decoded TPMS metrics, vehicle speed, as well as the reported signal metadata.

Fig. 2(a) illustrates three primary measurements decoded from a single TPMS sensor: vehicle speed, tire pressure, and temperature. The vehicle maintained highway speeds between 40–80 km/h with some variations, and the tire temperature exhibited a gradual, predictable increase from approximately 85°F to 95°F, correlating strongly with sustained vehicle speed. The pressure remained notably stable around 35 PSI with only minimal fluctuations throughout the drive. These highly predictable patterns in the primary TPMS parameters (stable pressure and temperature's correlation with speed) make them unsuitable as a source of entropy for key generation.

In contrast, Fig. 2(b) reveals more promising result. In the normalized noise components captured by two devices, the signals exhibit both significant temporal randomness and strong inter-device correlation, with a correlation coefficient of 0.89 between two devices (A and B). This combination of unpredictability and consistent correlation between independent receivers makes these noise patterns particularly suitable for key generation purposes. Moreover, the noise characteristics exhibit zero correlation with the predictable TPMS measurements shown in Fig. 2(a), suggesting a reliable source of environmental randomness for secure authentication.

From the captured noise, we developed a simple bit extraction method for generating authentication keys. Our approach analyzes the signal trend between consecutive samples: an increasing trend generates a bit value of `1`, while a decreasing trend produces a bit value of `0`. This way the exact amplitude and minor fluctuations, which can vary arbitrarily between receivers, does not affect the final comparison. Using this method, we consistently achieved *95%* bit agreement rate between legitimate in-vehicle devices over sequences of 500 bits. More importantly, devices positioned outside the vehicle achieved only approximately *50%* bit agreement rate (equivalent to random guessing), confirming the spatial security properties of our system. This observation validates that TPMS signal can serve as a robust source for generating shared keys between legitimate devices while maintaining security against external adversaries.

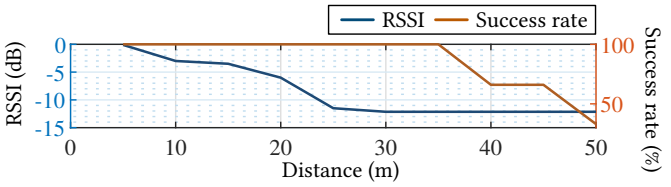

Fig. 3. Communication success rate and RSSI of TPMS sensor with respect to varying distance.

To evaluate the spatial security properties, we conduct distance-based measurements of TPMS sensor using two key metrics: received signal strength indicator (RSSI) and communication success rate (rate of successful packet delivery). We position our receiver at increasing distances from the sensor while collecting TPMS transmissions. As illustrated in Fig. 3, the RSSI decreased exponentially with distance, reaching -12 dB at 30 meters from the vehicle. More importantly, the communication success rate shows a clear security boundary—while devices achieve 100% success rate at 35 m, the rate drops to below 10% at 50 m. This natural signal attenuation creates an effective security boundary around the vehicle, making it difficult for attackers to replicate the authentication process from the outside.

III. Conclusion

Our experimental results demonstrate that while the primary TPMS measurements exhibit predictable patterns, the background noise and signal characteristics of RF transmissions shows promising potential as a source of environmental randomness. The high correlation of noise within the vehicle, combined with the rapid spatial decay of signal quality, suggests potential security applications in vehicular systems. Ongoing research efforts focus on two critical system improvements: increasing the bit generation rate beyond current TPMS transmission frequency limitations and implementing information reconciliation protocols to achieve 100% matching keys between legitimate devices while maintaining security against adversaries. Future work will also focus on developing more sophisticated noise extraction methods and evaluating the statistical quality of the generated random sequences across diverse environmental conditions. By leveraging readily available TPMS in all modern vehicles, these advances will enable lightweight, robust, and practical authentication for connected vehicles in the emerging shared mobility landscape.

ACKNOWLEDGEMENTS

This work was supported by the US Department of Transportation (USDOT) Tier 1 University Transportation Center (UTC) Transportation Cybersecurity Center for Advanced Research and Education (CYBER-CARE) (Grant No. 69A3552348332).

REFERENCES

[1] J. Han *et al.*, "Convoy: Physical context verification for vehicle platoon admission," in *ACM HotMobile*, 2017.
[2] K. Lee *et al.*, "ivpair: context-based fast intra-vehicle device pairing for secure wireless connectivity," in *ACM WiSec*, 2020.
[3] D. Schurmann and S. Sigg, "Secure communication based on ambient audio," *IEEE TMC*, 2013.
[4] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *PERVASIVE '07*, 2007.
[5] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *USENIX Security*, 2010.
[6] C. W. Zuckschwert, "RTL 433," https://github.com/merbanan/rtl_433.