7-2020

ivPair: context-based fast intra-vehicle device pairing for secure wireless connectivity

Kyuin Lee
University of Wisconsin

Neil Klingensmith
Loyola University Chicago, nklingensmith@luc.edu

Dong He
University of Wisconsin

Suman Banerjee
University of Wisconsin

Younghyun Kim
University of Wisconsin

Recommended Citation

Lee, Kyuin; Klingensmith, Neil; He, Dong; Banerjee, Suman; and Kim, Younghyun. ivPair: context-based fast intra-vehicle device pairing for secure wireless connectivity. WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, , : 25-30, 2020. Retrieved from Loyola eCommons, Computer Science: Faculty Publications and Other Works, http://dx.doi.org/10.1145/3395351.3399436

ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity

Kyuin Lee*, Neil Klingensmith§, Dong He*, Suman Banerjee*, and Younghyun Kim*
*University of Wisconsin–Madison and §Loyola University Chicago
*{kyuin.lee, dhe28, younghyun.kim}@wisc.edu, §neil@cs.luc.edu, *suman@cs.wisc.edu

Abstract

The emergence of advanced in-vehicle infotainment (IVI) systems, such as Apple CarPlay and Android Auto, calls for fast and intuitive device pairing mechanisms to discover newly introduced devices and make or break a secure, high-bandwidth wireless connection. Current pairing schemes are tedious and lengthy as they typically require users to go through pairing and verification procedures by manually entering a predetermined or randomly generated pin on both devices. This inconvenience usually results in prolonged usage of old pins, significantly degrading the security of network connections.

To address this challenge, we propose ivPair, a secure and usable device pairing protocol that extracts an identical pairing pin or fingerprint from vehicle's vibration response caused by various factors such as driver's driving pattern, vehicle type, and road conditions. Using ivPair, users can pair a mobile device equipped with an accelerometer with the vehicle's IVI system or other mobile devices by simply holding it against the vehicle's interior frame. Under realistic driving experiments with various types of vehicles and road conditions, we demonstrate that all passenger-owned devices can expect a high pairing success rate with a short pairing time, while effectively rejecting proximate adversaries attempting to pair with the target vehicle.

CCS Concepts

• **Human-centered computing** → **Ubiquitous and mobile computing systems and tools**; • **Security and privacy** → *Authentication.*

Keywords

Device pairing; device authentication; pin generation

ACM Reference Format:
Kyuin Lee, Neil Klingensmith, Dong He, Suman Banerjee, and Younghyun Kim. 2020. ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3395351.3399436

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399436

1 Introduction

With the prevalence of mobile devices with miniaturized form factors and limited user-interfaces, such as smart watches and wireless earbuds, there is an increasing need for a new pairing mechanism to spontaneously and securely authenticate newly introduced devices to an existing network. For instance, connecting a mobile device to an in-vehicle infotainment (IVI) system has long been a problem that is much more bothersome than it sounds. To do this, the user has to navigate through multiple steps to discover the device to pair and enter a randomly generated pin to verify the device's authenticity. This pairing process is often tedious and lengthy, and sometimes not so user-friendly and unsafe to do while driving that it even discourages users from using it unless the pairing purpose is expected to have a long lifetime. When the pairing procedure is deemed necessary, since this inconvenient procedure is not considered to be an everyday task, the vehicle's on-board computer system would remember the paired device and reuse the pre-negotiated pin, which can be vulnerable to number of attacks [3].

Unfortunately, this pairing mechanism remains surprisingly outdated in spite of the emerging advanced IVI systems, such as Apple CarPlay and Android Auto, that acts more like a smartphone embedded in the car. As the sensitivity of personal data exchanged within the network is much more higher than just an audio playback or personal contact information, today's IVI systems demand higher level of security than conventional car audio systems. Additionally, the utility of such systems would be maximized by inter-operating with mobile devices, often not only the driver's device but also (sometimes anonymous) passengers' devices with short-lived pairing. To meet this emerging demand, a secure and usable mechanism for spontaneous pairing is required to eliminate the inconveniences of conventional methods.

As a promising solution to enable fast and convenient yet secure device authentication, *context-based authentication* has recently emerged [4]. The *coexistence* of two (or multiple) devices is verified by comparing a random key or pin independently generated from an ambient source of randomness, such as wireless signal strength [13], luminosity and acoustic noise [15, 19]. Because of the pervasive and continuous nature of randomness in such ambient sources, it prevents the risk of using poorly chosen passwords over a long period across multiple pairs of devices. Due to its high security and convenience, it has been studied to replace conventional authentication methods or be used in tandem to augment it.

In this paper, we propose a secure and usable pairing protocol to extract entropy from the road conditions to automatically generate authentication pins for multiple devices within the same car. While *mechanical vibration* has been used in some previous work for device pairing [7, 11] due to ubiquitous presence of accelerometers in today's mobile devices (e.g., smartwatches, smartbands, and

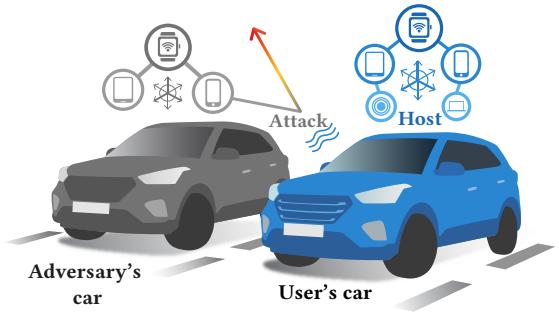

Figure 1: Passenger-owned mobile devices in the legitimate user's vehicle are pairing with the vehicular computer (host).

smartphones), there has been little investigation in the context of in-vehicle usage. More specifically, this paper investigates the use of vibration simultaneously measured by a vehicular computer and a mobile phone in the same vehicle to subsequently establish a secure wireless connection (e.g., Bluetooth or Wi-Fi) between them. The contributions of this paper are as follows:

- We present an intra-vehicle device pairing protocol called ivPair, which exploits simultaneously measured vibration to generate a common pin to establish a secure wireless connection.
- We design and implement integral techniques to overcome challenges in realizing ivPair on commercial mobile devices, such as lack of time synchronization and sampling frequency mismatch.
- We conduct real-world experiments under various driving environments and demonstrate successful pin generation and its robustness against adversaries.

2 System Models

The assumptions and system models of ivPair, including its threat model, are as follows.

System model: We consider a scenario where passenger-owned mobile devices within a vehicle are trying to establish a secure high-bandwidth wireless connection (e.g., Bluetooth or Wi-Fi) to the vehicle's computer system by generating identical pins while the vehicle is actively in motion, as illustrated in Figure 1. We assume that there exists an on-board reference accelerometer attached within the center console of the host vehicle.

Threat model: To be considered as a secure pairing scheme, some common attack scenarios need to be taken into account. We assume an active adversary that is maliciously or unintentionally trying to pair with the legitimate victim's vehicle or their mobile devices to tamper with or control the system. The adversary does not have direct physical access and is not present within the victim's vehicle but knows the type of the car and can drive closely to the victim within its wireless range. Additionally, we assume that the adversary can eavesdrop on any plaintext wireless messages that are used in the legitimate pairing process.

3 Proposed Pairing Protocol

In this section, we present the overall protocol of ivPair to pair two devices with no prior knowledge.

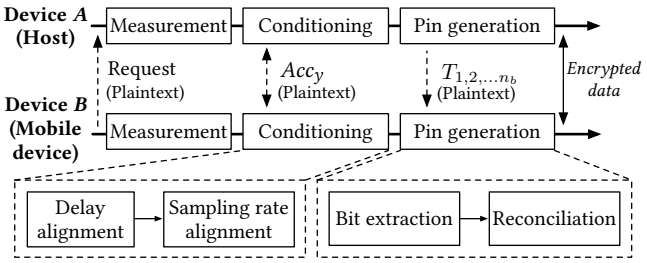

Figure 2: Overall protocol to extract identical pins on two devices to bootstrap high-bandwidth wireless connection.

3.1 Overview

The only additional hardware component required by ivPair is a reference accelerometer embedded in vehicle in the direction parallel to the car, with y-axis pointing towards the direction of travel and z-axis pointing downwards through the chassis. To pair with a mobile device on the go, the user simply holds the device (embedded with an accelerometer) against the moving vehicle's interior door frame closest to his/her sitting position.

Figure 2 illustrates the pairing process, which consists of three phases: i) measurement, ii) conditioning, and iii) pin generation. To initiate pairing, Device B (user's mobile device) transmits a pairing request to Device A (host vehicle), and both devices independently measure its own acceleration in y- and z- axes. For simplicity, we assume that the user contacts the accelerometer of the mobile device oriented the same direction as the reference accelerometer since the orientation of two accelerometers observing identical linear acceleration in two orthogonal directions can be easily aligned [2, 21]. Following the conditioning and pin generation phases, the two devices generate identical pins to communicate through a secure encrypted channel. Note that all information exchanged between two devices until the completion of the pin generation phase is in plaintext that can be eavesdropped by the adversary.

3.2 Measurement and conditioning

The main source of entropy to generate a pin is the vibration response of the moving vehicle perpendicular to the direction of travel. That is, the acceleration signal from z-axis, $Acc_{z,u}$, is utilized to extract pins from both devices, where u denotes one of the devices, A or B. However, the raw measurement cannot be directly used to extract bits due to significant temporal misalignment caused by: i) time offset resulting from the transmission delay of the pairing request message and ii) sampling frequency mismatch caused by variation between the devices. To achieve temporal alignment without revealing secret, two devices leverage the acceleration in y-axis, $Acc_{y,u}$, which represents the vehicle's linear acceleration towards the direction of travel resulting from the driver's behavior of accelerating and breaking. Note that, since Acc_y is more predictable by an external observer, it is used for signal conditioning only, but should not be used for actual pin generation.

More specifically, the devices utilize the sliding window approach to find the index of a sample that exhibits the highest correlation between its own Acc_y and the other's Acc_y. However, while this process may synchronize the starting points, the sampling rate variation between the devices results in additional misalignment as

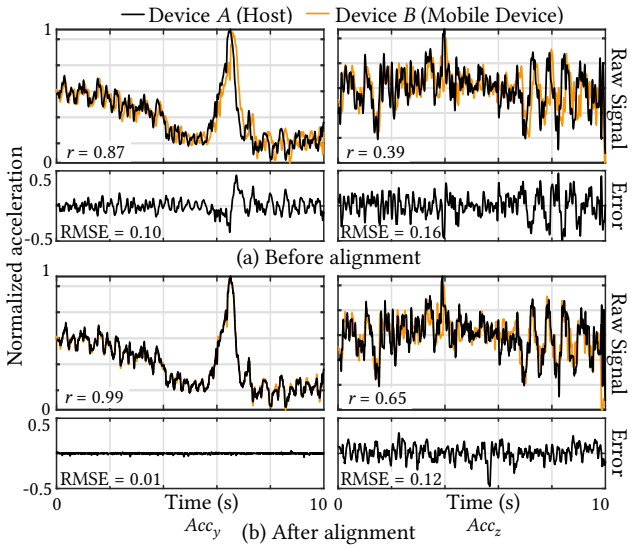

Figure 3: Measured Acc_y and Acc_z, sample-wise error, and correlation coefficient r between two devices (a) before and (b) after sampling frequency alignment using DTW.

the number of measurements accumulate. Therefore, after aligning the starting points, we correct the sampling frequency discrepancy by adopting dynamic time warping (DTW) [1] on synchronized $Acc_{y,A}$ and $Acc_{y,B}$ to calculate the optimal correspondence between them. Each device extracts its non-linear warping path i_A and i_B which represents the indices of $Acc_{y,A}$ and $Acc_{y,B}$ with minimum distance with respect to each other. Then the devices independently apply their warping path i_A and i_B on $Acc_{z,u}$, to obtain tightly aligned fingerprints F_u with respect to each device.

Figure 3 compares Acc_y and Acc_z measured from two devices and their sample-wise error before and after the proposed signal conditioning. As shown in Figure 3(a), without the DTW-based alignment, two signals on both axes are severely misaligned even within a 10-s measurement. The sample-wise error plot shows that the magnitude of the error gradually increases as the sampling time increases, due to the sampling frequency variation between two devices. On the other hand, after they are aligned using the warping path calculated from Acc_y, as illustrated in Figure 3(b), the error rate of two axes is drastically reduced (from root mean square error (RMSE) of 0.10 to 0.01, and 0.16 to 0.12, respectively), resulting in a significant improvement in correlation between $Acc_{z,A}$ and $Acc_{z,B}$ from 0.39 to 0.65.

3.3 Pin generation

The two time-aligned fingerprints F_u obtained by two devices are the main source of randomness to harvest identical bit sequences. To quantize F_u into bit sequences K_u, we employ the noise-based random bit generation method [10], where time-series fingerprint signals are uniformly segmented into several subsections n_b, and the index of the maximum absolute value, T_b, in each subsection is exchanged to be converted into bits. If the signal value at each index is greater than the mean of the subsection, a bit 1 is extracted; otherwise a bit 0 is extracted. Because there exists no periodic nature in the high-frequency components of F_u, we segment the entire fingerprint into n_b subsections which represents the number of extracted bits and extract bits as follows:

$$K_{u,b} = \begin{cases} 1 & \text{if } F_{u,b}(T_b) \geq \text{mean}(F_{u,b}) \\ 0 & \text{if } F_{u,b}(T_b) < \text{mean}(F_{u,b}). \end{cases} \quad (1)$$

This bit extraction scheme results in nearly identical sequences but may exhibit occasional bit errors due to remaining timing mismatch. To resolve these errors without leaking any information about the pin itself, the following reconciliation phase utilizes error-correcting code (ECC) to map equivalently segmented bit sequences to one of the pre-computed codewords. For instance, when using Hamming(n, k) as a base ECC, the results of equally segmented n-bits from the bit extraction phase will map to a n-bit codeword that exhibits the minimum Hamming distance.

4 Implementation and Evaluation

In this section, we evaluate ivPair under realistic usage and adversarial scenarios.

4.1 Experimental setup and metrics

We evaluate the performance of ivPair with different body types of vehicles driven on various types of roads. In total, more than 3-hour worth of real-world driving data is collected using triple-axis ADXL345 MEMS accelerometer connected to Arduino Uno boards at a sampling frequency of 800 Hz. For each pairing attempt, 10-s long accelerometer measurement is used to extract 14-bit pins. We employ Hamming(7, 4) as the ECC for reconciliation to resolve bit errors. To simulate the user holding the mobile device against the interior panel of the vehicle, we use adhesive tape to fix a reference accelerometer (representing the host) to the center console as well as different positions within the car. For all driving environments, the driver maintained safe driving behavior without any aggressive or abrupt accelerating and breaking activities to intentionally improve signal-to-noise ratio.

We primarily focus on two evaluation metrics: the *bit agreement rate* and the *success rate* of pairing attempts. Bit agreement rate refers to the rate of equal bit-wise comparison results between two generated pins before reconciliation, and success rate represents the rate of successful pairing that exhibits a perfect (100%) bit agreement rate after reconciliation. Additionally, as a measure of user experience accounting for pairing failure scenarios, we define *expected pairing time* to be inversely proportional to the success rate times the duration of the measurement (10 s).

4.2 Bit randomness

First, in order to investigate the quality of bit sequences generated from the ivPair, we record the histogram of the frequency of bit 1's in the generated bit sequences. To prevent an adversary from randomly guessing the pin, a high-quality pin should contain statistically equal number of bit 0's and 1's. If the sequence dominantly embeds more number of 1's than 0's or vice-versa (i.e., biased), the contexts that are used for the fingerprint extraction is not considered ideal.

Since ivPair determines each bit by the relative magnitude of random noise and the mean value based on (1), the probability

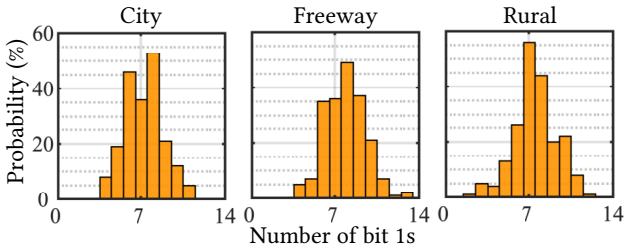

Figure 4: Histogram of 14-bit pin sequences based on their number of bit 1s.

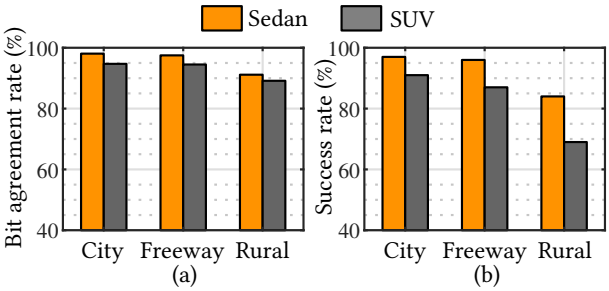

Figure 5: (a) Bit agreement rates and (b) success rate on sedan and SUV driven on different roads.

of appearance of a bit 1 and a bit 0 are equally likely. Ideally, in the case of a 14-bit pin sequence, the number of bit 1's should be around 7 to indicate frequent contextual changes within the measured fingerprint signals. Figure 4 illustrates the histogram of 100 sequences generated from the city, highway and suburb driving conditions. All three distributions exhibit a binomial distribution centered around 7 with no sequence that exhibits continuous 0s or 1s, which indicates the presence of entropy and randomness in the fingerprints that makes it difficult for the adversary to randomly guess the established pin.

4.3 Vehicle and road types

Different vibration responses resulting from different types of vehicles, roads, and traffic conditions can affect the overall pairing process. In order to investigate these variations, we conduct experiments using a sedan and a sport utility vehicle (SUV) driven on the city, freeway and rural roads. One accelerometer fixed to the driver side door frame is requesting to pair with the host fixed to the center front console. For each road type, 100 pairing attempts are made. Overall, as Figure 5(a) illustrates, both types of vehicles show high bit agreement rates. In particular, the sedan type vehicle achieves 98.1% bit agreement rate in the city, while the SUV type exhibits 95.0%. This is due to the fact that the higher chassis and clearance height of the SUV results in a higher sensitivity to road and traffic conditions that leads to a slight difference in vibration responses between two devices. The results also show overall high bit agreement rates for all types of roads, close to exceeding 90%. Rural driving exhibits slightly lower agreement rates in both vehicle types compared to the freeway and city driving due to unstable

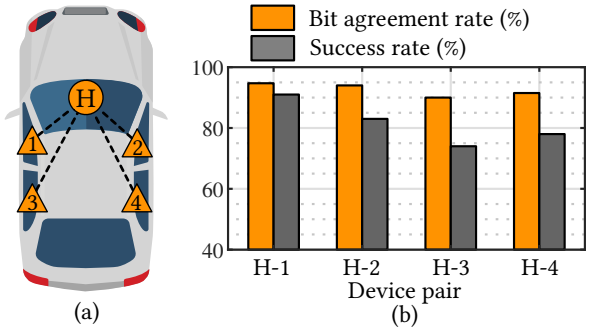

Figure 6: (a) Location of devices (H: host, 1–4: mobile devices). (b) Pairing success rate and bit agreement rate between pairs of devices.

accelerometer data from frequent and larger bumps and cracks on unpaved road surfaces. As illustrated in Figure 5(b) the high bit agreement rates lead to high success rates above 85% for all freeway and city driving in both vehicle types. While the SUV case in rural driving shows the lowest success rate out of all cases at around 69%, city driving exhibits high success rates of 97% and 91% for the sedan and SUV, respectively. These results indicate that even under variations caused by different roads and vehicle types, a high success rate is maintained at 87% on average.

4.4 Location of mobile devices

Next, we investigate the performance of ivPair at varying locations within the vehicle. Figure 6(a) shows the locations of the host as well as other mobile devices' location. For each device pairs, 100 pairing attempts are made on the city roads. Figure 6(b) shows the bit agreement rate and the pairing success rate for four different location pairs. The devices placed in the front seats, closer to the host accelerometer, show an average agreement rate of 94.7% and 94.0% for the driver side (H-1) and the passenger side (H-2), respectively. The devices that are located in the rear seats achieve slightly lower agreement rates due to the natural location variation that leads to a slight difference in its fingerprints. However, our experiments suggest all the passengers in the vehicle will experience an acceptable success rate of above 70% with a mean of 85%, regardless of their seat position.

We also show that ivPair's conditioning process (DTW-based sampling frequency alignment) significantly improves the correlation between fingerprints generated by device pairs. As presented in Table 1, all fingerprint pairs exhibit low mean correlations (0.15 on average) before conditioning. However, after conditioning, the mean correlations are dramatically improved to 0.71 on average, enabling successful pairing at a high probability.

A low success rate due to unresolved bit error after reconciliation means that the device has to repeatedly attempt to pair with the host, which directly degrades the user experience due to long pairing time. Specifically, a user sitting in the driver side of the car (the Host-1 pair) can expect an average pairing time of 11.0 s thanks to the higher success rate as compared to other location pairs. For passengers sitting in rear seats, it will take 13.5 s on average. Overall, regardless of their sitting positions, all the users within the same

Table 1: Expected pairing time and mean correlation coefficient before and after conditioning.

Device pair	Correlation coefficient	Expected time
Host-1	0.11 → 0.79	11.0 s
Host-2	0.06 → 0.78	12.0 s
Host-3	0.32 → 0.65	13.5 s
Host-4	0.09 → 0.61	12.8 s

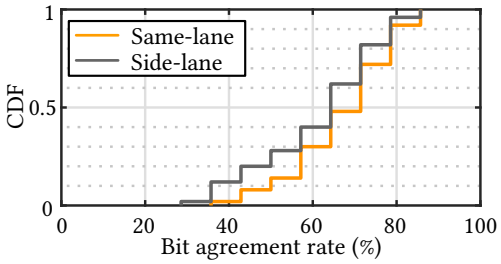

Figure 7: Bit agreement rate achieved by the adversary under two different attack scenarios.

vehicle can expect a reasonably short expected pairing time of less than 14 s.

4.5 Adversarial scenarios

We consider two adversarial attack scenarios according to our threat model where we assume that the legitimate vehicle is within the sight of the adversary. The *same-lane* scenario is where the adversary is actively driving with the target vehicle in the same lane. To maximize the adversary's bit agreement rate against the victim vehicle, the adversary is driving in front of the victim vehicle and delays its measured fingerprint signal to account for slight timing difference caused by the distance between two vehicles. Additionally, in the *side-lane* scenario, the adversary is driving the car side-by-side in a multi-lane road. We conduct this experiment with two sedan vehicles within the city driving condition and assume that the adversary is equipped with identical accelerometer hardware as the victim. In total, the adversary attempts 50 pairing requests in each scenario, utilizing the acceleration measured from the adversary's vehicle. The bit agreement rates resulting from the two attack scenarios are presented in Figure 7. Overall, the adversary conducting the side-lane attack is able to achieve a mean bit agreement rate of 61.3% compare to the legitimate pin. The adversary was able to guess only up to 85.7% of the legitimate key in two out of 50 attempts before reconciliation, which is below the threshold to pair with the victim vehicle. On the other hand, in the same-lane attack scenario, the adversary achieves a slightly higher mean bit agreement rate of 70%. This is because the adversary mimicking the legitimate fingerprint in the same-lane is more likely to experience the same bumps and cracks than in the side-lane scenario. However, under both attack scenarios, none of the attempts successfully pairs with the victim's vehicle.

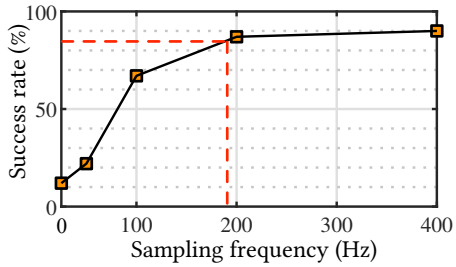

Figure 8: Pairing success rate with respect to the sampling frequency of devices.

4.6 Sampling frequency analysis

Generally, the higher the sampling frequency, the better the accuracy to capture the vehicle's vibration responses, which increases the overall bit agreement and pairing success rates. Therefore, in order to examine the minimum sampling frequency to maintain a reasonable success rate, we downsample the measured fingerprints from 800 Hz down to 25 Hz and attempt to pair a device attached to the driver's door panel (H-1 pair in Figure 6). As illustrated in Figure 8, the success rate is maintained above 85% as long as the sampling frequency is greater than 200 Hz. As the frequency reduces to below 200 Hz, the success rate starts to decrease. Specifically, frequency of 50 and 25 Hz exhibit success rate of 22% and 12%, respectively, significantly degrading the usability of ivPair. Therefore, to maintain an acceptable success rate higher than 80%, which corresponds to an expected pairing time of 12.5 s, the sampling frequency must be kept above around 170 Hz. Most modern mobile devices are equipped with MEMS accelerometers that can easily meet this sampling frequency requirement.

4.7 Computational overhead of DTW

The main computational overhead of ivPair is the execution of DTW algorithm in the signal conditioning phase to achieve sampling rate alignment. In order to validate the feasibility of computing DTW on commercial mobile devices, we implement an Android application running on LG Nexus 5X (Android 5.0) with 1.8 GHz processor, which is a mid-range smartphone nowadays, and measure the algorithm's computational run time. The application takes in two discrete time series of 8,000 samples (10-s long fingerprint at 800 Hz) and matches the samples of one series to another. On average, computing the alignment path takes only 564 ms, which indicates that the computational overhead does not significantly affect the usability of ivPair.

5 Discussion

In this section, we further discuss remaining challenges and future directions of ivPair.

Vehicle must be in motion: For ivPair to work, we need a common source of linear acceleration in one direction to obtain tightly synchronized fingerprints, which requires the vehicles to be in motion. This requirement makes ivPair slightly constrained in terms of its usability to pair anytime. However, considering that the need for a convenient device pairing method is more imperative

when the driver should not be distracted, ivPair would be useful in practical scenarios.

Entropy vs usability trade-off: In our evaluation, we found that it takes about 10 s to extract a 14-bit pin—roughly the same amount of information as in a four decimal-digit Bluetooth pin. If the length of bits extracted increases, the bit agreement rate would decrease due to the differences in the fingerprints caused by sensor variation and locality. Therefore, further investigation is needed in order to evaluate the trade-off between security (bit length) and usability (expected pairing time).

Human factors: Ideally, the pairing process should be seamless—the user should be able to pair a device while holding it in their hand or in the pocket. To deal with this problem, we could treat the user's body—including the seat and their hand grasping the phone—as a linear time-invariant system that filters bumps from the road before the bumps can be measured by the device's accelerometer. Additionally, our experiments are conducted in the vehicle with no background audio or music. We imagine that loud sounds can cause the door frames to vibrate since the speakers are usually embedded in the frames.

6 Related Work

Context-based pairing and authentication have actively been studied to leverage various ambient contextual information that can be measured by rich sensing capabilities on today's mobile and stationary IoT devices. Specifically, devices deployed in homes and offices can leverage various surrounding physical contexts to mutually authenticate colocated devices. For example, measurements from ambient audio, received signal strength indicator (RSSI), visual channel and luminosity can be used to generate identical keys to establish secure communication channel [13, 15, 17, 19]. Additionally, [4] provides first large-scale public dataset of various devices in multiple environments (i.e., car and office) and re-evaluates various zero interaction pairing and authentication schemes.

In the wearable and mobile device domain, identical keys for pairing can be extracted from the legitimate user's electrocardiography (ECG) signal by extracting the time interval between two consecutive peaks from piezo or ECG sensors [12]. To authenticate multiple mobile devices carried by the walking user, [11, 21] proposes key generation method from walking characteristics (gait) of the user based on their acceleration signal from different parts of their body. As an interactive pairing method, [14] proposes device-to-device authentication by letting the user simultaneously shake two devices and use its movement patterns for key generation purposes.

Mechanical vibration context has proven to be useful for establishing a common secret only between colocated devices thanks to its proximity nature and the ubiquitous availability of accelerometers in various devices. Much like NFC and ultrasound [8, 20], it can be used as an out-of-band communication channel to explicitly transmit and receive data using a vibration generator and an accelerometer [7, 9, 16, 18], but it requires the devices to be in direct physical contact to transfer a secret generated by one device to another. Relevant research proposes to use vibration measured by multiple vehicles in the same lanes (a platoon of vehicles) to authenticate a newly joining vehicle for vehicle platooning purposes [6]. Recently, [5] addressed secure pairing of devices within multi-modal transport (i.e., train, tram, bike, and vehicle). Compared to this work, we specifically focus on the vehicular application with extensive experiments including adversarial attacks and multiple device locations under various road conditions and achieve consistently higher pairing success rates.

7 Conclusion

We proposed a fast and convenient method for pairing devices within the same vehicle, called ivPair. The results from extensive experiments show that ivPair can complete device pairing within a reasonable time at a high success rate in various vehicle types and road conditions as validated with extensive real-world experiments. It is shown that it can successfully reject nearby adversaries in the same or next lane. The proposed method would enable seamless connection between mobile devices and emerging IVI systems, potentially facilitating innovative mobile applications with short-lived device pairing.

Acknowledgements

This work was supported by the Wisconsin Alumni Research Foundation and NSF under grants CNS-1719336 and CNS-1845469. Neil Klingensmith and Suman Banerjee were supported in part through the following US National Science Foundation grants: CNS-1838733, CNS-1719336, CNS-1647152, and CNS-1629833.

References

[1] Donald J. Berndt and James Clifford. 1994. Using Dynamic Time Warping to Find Patterns in Time Series. In *AAAIWS '94.*
[2] Chongguang Bi and Guoliang Xing. 2018. Real-Time Attitude and Motion Tracking for Mobile Device in Moving Vehicle. In *ACM SenSys '18.*
[3] John Dunning. 2010. Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security and Privacy* 8 (March 2010).
[4] Mikhail Fomichev et al. 2019. Perils of Zero-Interaction Security in the Internet of Things. *ACM IMWUT 3* (2019).
[5] Bogdan Groza et al. 2020. Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport. *IEEE Access* 8 (2020).
[6] Jun Han et al. 2017. Convoy: Physical Context Verification for Vehicle Platoon Admission. In *ACM HotMobile '17.*
[7] Younghyun Kim et al. 2015. Vibration-Based Secure Side Channel for Medical Devices. In *ACM/EDAC/IEEE DAC '15.*
[8] Tim Kindberg and Kan Zhang. 2003. Validating and Securing Spontaneous Associations between Wireless Devices. In *ISC '03.*
[9] Kyuin Lee et al. 2018. SYNCVIBE: Fast and Secure Device Pairing through Physical Vibration on Commodity Smartphones. In *IEEE ICCD '18.*
[10] Kyuin Lee et al. 2019. VoltKey: Continuous Secret Key Generation Based on Power Line Noise for Zero-Involvement Pairing and Authentication. *ACM IMWUT 3* (2019).
[11] Jonathan Lester et al. 2004. "Are You with Me?" – Using Accelerometers to Determine If Two Devices Are Carried by the Same Person. In *PERVASIVE '04.*
[12] Qi Lin et al. 2019. H2B: Heartbeat-Based Secret Key Generation Using Piezo Vibration Sensors. In *ACM/IEEE IPSN '19.*
[13] Suhas Mathur et al. 2011. ProxiMate: Proximity-Based Secure Pairing Using Ambient Wireless Signals. In *ACM MobiSys '11.*
[14] Rene Mayrhofer and Hans Gellersen. 2007. Shake Well Before Use: Authentication Based on Accelerometer Data. In *PERVASIVE '07.*
[15] Markus Miettinen et al. 2014. Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices. In *ACM CCS '14.*
[16] Nirupam Roy and Romit Roy Choudhury. 2016. Ripple II: Faster Communication through Physical Vibration. In *USENIX NSDI '16.*
[17] Nitesh Saxena et al. 2006. Secure Device Pairing Based on a Visual Channel (Short Paper). In *IEEE S&P '06.*
[18] Nitesh Saxena et al. 2011. Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags. In *IEEE PerCom '11.*
[19] Dominik Schurmann and Stephan Sigg. 2013. Secure Communication Based on Ambient Audio. *IEEE TMC* (2013).
[20] Roel Verdult and Francois Kooman. 2011. Practical Attacks on NFC Enabled Cell Phones. In *NFC '11.*
[21] Weitao Xu et al. 2016. Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure on-Body Device Communication. In *ACM/IEEE IPSN '16.*