2015 International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing, Networking and Communications (CNC)

The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks

Bastian Bloessl[†], Christoph Sommer[†], Falko Dressler[†] and David Eckhoff[*]
[†] Distributed Embedded Systems Group, Dept. of Computer Science, University of Paderborn, Germany
[*] Computer Networks and Communication Systems, Dept. of Computer Science, University of Erlangen, Germany
{bloessl,sommer,dressler}@ccs-labs.org, eckhoff@cs.fau.de

***Abstract*—Vehicular networks provide the basis for a wide range of both safety and non-safety applications. One of the key challenges for wide acceptance is to which degree the drivers' privacy can be protected. The main technical privacy protection mechanism is the use of changing identifiers (from MAC to application layer), so called pseudonyms. The effectiveness of this approach, however, is clearly reduced if specific characteristics of the physical layer (e.g., in the transmitted signal) reveal the link between two messages with different pseudonyms. In this paper, we present such a fingerprinting technique: the scrambler attack. In contrast to other physical layer fingerprinting methods, it does not rely on potentially fragile features of the channel or the hardware, but exploits the transmitted scrambler state that each receiver has to derive in order to decode a packet, making this attack extremely robust. We show how the scrambler attack bypasses the privacy protection mechanism of state-of-the-art approaches and quantify the degradation of drivers' location privacy with an extensive simulation study. Based on our results, we identify additional technological requirements in order to enable privacy protection mechanisms on a large scale.**

I. Introduction

Inter-Vehicle Communication (IVC) supports the exchange of messages between cars and also with infrastructure nodes such as access points called Roadside Units (RSUs). Even though the topic gained a lot of attention by both industry and academia, several important challenges still need to be addressed [1]. Vehicular networks can provide a wide range of safety [2] and non-safety [3] applications. Decentralized ad hoc networks, i.e., Vehicular Ad Hoc Networks (VANETs) based on Dedicated Short-Range Communication / Wireless Access in the Vehicular Environment (DSRC/WAVE) and IEEE 802.11p, are considered a key technology for cooperative vehicular safety [4] and in early 2014 the U.S. National Highway Traffic Safety Administration announced a push towards bringing DSRC/WAVE technology on the road.

It is beyond dispute that this technology has many advantages – however, serious privacy concerns still remain [5]. By overhearing the unencrypted periodic beacon messages of vehicles, it is possible for operators of, e.g., networks of RSUs to track drivers through the network and reveal their locations [6]. To counter this, both the European and the U.S. system dictate the use of a Public Key Infrastructure (PKI) employing pseudonymous identifiers, which have to be signed by a certificate authority and cannot be linked to the real identity of a driver by anyone else [7], [8]. Location privacy is then achieved by frequently changing these pseudonyms (along with all other identifying information such as the MAC address). The goal is to make it impossible to track vehicles by linking messages with different pseudonyms to each other.

Privacy is becoming a critical concern also in the WiFi domain. The use of privacy preservation techniques has for example been integrated in new Apple products where MAC addresses are randomized during the active probing for new base stations. This trend will continue with new wearable devices. In the scope of this paper, however, we primarily focus on vehicular networks as a base technology.

Attack vectors to still link messages despite changing identifiers usually include the exploitation of physical layer characteristics, e.g., unique features of the electromagnetic waveform emitted by a particular transceiver. However, such approaches need to rely on potentially fragile features of the channel or the hardware. Thus, they are unlikely to work well in highly dynamic vehicular networks.

In this paper, we reveal and discuss a novel attack vector based on data contained directly in the physical layer: the scrambler state. Scrambling, despite its name, is not related to network security but is an important process to improve wireless communication performance. An attack exploiting this mechanism becomes possible by employing a Software Defined Radio (SDR) rather than Commercial Off The Shelf (COTS) hardware, as these transceiver chips do not disclose the necessary information. Conversely, an SDR allows an attacker free access to the complete physical layer frame. We identified a robust passive fingerprinting technique based on non-random initial scrambler states that can be exploited to considerably degrade the location privacy of vehicles and, thus, their drivers.

Using our Open Source SDR-based IEEE 802.11a/g/p transceiver presented in [9], we were able to gain access to this information and reverse engineer the scrambler algorithms of current IEEE 802.11p prototypes and COTS hardware. We present our investigation of the weakness of these algorithms as well as the results of an extensive simulation study of best/worst case scenarios of an attacker attempting to track vehicles across an intersection and through blind spots in radio coverage. This allows us to give a quantitative indication of the impact of the presented attack vector.

Our contributions can be summarized as follows:

- We present a novel attack on location privacy that tremendously simplifies the re-identification of WiFi and IEEE 802.11p devices. This attack targets physical layer

978-1-4799-6959-3/15/$31.00 ©2015 IEEE

characteristics at a late stage (on bit level), rather than signal characteristics, so it needs no calibration and is highly robust to channel or hardware variations.
- We demonstrate the applicability of this attack in practice, using both prototype and COTS hardware that is in widespread use either in current Field Operational Tests (FOTs) investigating IVC applications, or in our laptop computers that we use to connect to WiFi hotspots.
- We gauge the impact of the attack based on best/worst case simulation studies, showing that this technique has the potential to completely undermine current efforts to ensure privacy.

The remainder of the paper is organized as follows: We discuss the state of the art in physical layer fingerprinting as well as its applicability in vehicular environments in Section II. In Section III we present our novel attack vector on location privacy and discuss the vulnerability of current hardware in Section IV. We discuss the implications of this attack in Section V, then give a quantitative estimation of its impact by means of a simulation study in Section VI. We conclude the paper after discussing potential countermeasures in Section VII.

II. Related Work

Due to their large success, IEEE 802.11 networks gained much interest from the research community. When these devices become mobile, as it is the case in vehicular networks but also with WiFi-enabled mobile phones, the preservation of location privacy is a non-trivial challenge. On the physical layer, several attack vectors to track users' mobility have been identified and countermeasures have already been discussed [10]. Most of these attacks on IEEE 802.11 networks can be directly applied to IEEE 802.11p networks (i.e., the amendment for vehicular communication), however, their feasibility in highly dynamic environments such as vehicular networks has to be reconsidered.

On the physical layer, characteristic distortions of the physical waveforms of the signal can be exploited to re-identify a user. These distortions can be introduced by the wireless channel [11] or by imperfections and variations of the analog part of the hardware [12], [13]. Klein et al. present a method to identify WiFi devices with the help of characteristic features of the preamble by using a sophisticated signal analyzer using a static setup in a shielded chamber [14]. However, in highly mobile networks, like VANETs, where the signal is greatly influenced by effects of the wireless channel, these specific characteristics might be difficult to detect.

Ureten et al. show how the transient phase of IEEE 802.11b network cards, another feature of the physical waveform, can be exploited to identify a device with an accuracy of up to 98 % [15]. During the transient phase, i.e., immediately after the network card switched to transmit mode, the signal has a characteristic shape, which is induced by powering up transmit components like amplifiers. Even though this approach is very reliable in static scenarios, its practical exploitation in vehicular environments has yet to be shown.

Kohno et al. show how unique clock drift characteristics of a device can be exploited using timestamps of TCP packets [16]. This attack might also be applicable in VANETs as periodic beacon messages include a millisecond timestamp. However, vehicles in VANETs are equipped with GPS receivers that allow to derive the time with very high precision, possibly limiting the applicability of this method.

Another fingerprinting technique is the utilization of features of higher layers like protocol and traffic characteristics. Franklin et al. show how small, vendor specific implementation details can be used to identify the used hardware [17]. A limitation of these methods is that they do not identify a specific user, but disclose the model or vendor of the hardware. The scrambler attack presented in this paper is able to specifically identify a unique user with high probability, because even though the same hardware might be used by different users, their state differs.

III. Description of the Attack Vector

Frame encoding in IEEE 802.11a/g/p OFDM physical layers [18] is a rather complex process. However, for our attack, only a small part is relevant: the scrambler.

Note that (despite its name) scrambling is not a security or confidentiality feature: It was added to increase the performance of the physical layer.

The function of the scrambler is defined in IEEE 802.11 as follows: The binary payload of a frame is scrambled just before forward error correction is applied. With scrambling, the input data is xor'd with a pseudo random sequence, generated by a linear feedback shift register as depicted in Figure 1. This produces an uncorrelated binary sequence with uniformly distributed bits, maximizing the entropy and, thus, information content.

In Orthogonal Frequency Division Multiplexing (OFDM) systems, the scrambler has another advantage besides maximizing the information content of the input data: Since the scrambler generates a different pseudo random sequence per frame, the same data payload is mapped to different binary sequences and thus, physical signals. This is desirable, especially with OFDM, since certain bit patterns are mapped to disadvantageous waveforms with very high Peak to Average Power Ratio (PAPR) [19]. Without a scrambler, the same payload would always generate the same physical wave form. Therefore, certain payloads could experience systematically higher packet error rates.

The output of the scrambler depends only on its initial seed. According to the standard, the scrambler should be

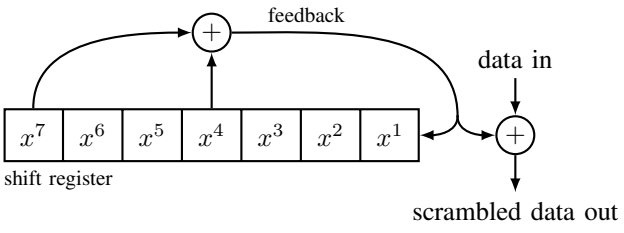


Figure 1. Schematic overview of the IEEE 802.11 scrambling algorithm.

seeded randomly with a nonzero value for every frame. More precisely, it states: "When transmitting, the initial state of the scrambler shall be set to a pseudo random nonzero state" [18, Section 18.3.5.5].

The receiver can reverse this process to decode the packet since the transmitter prefixes the payload with seven zeros. With these seven scrambled zeros the receiver can reconstruct the seven bits of the linear feedback register.

The seeding of the scrambler piqued our interest, as it might allow for an attack vector: If it were possible to correlate scrambler state seeds across multiple messages, this would allow for the re-identification of devices, and thereby drivers. Furthermore, such an attack would be highly robust against channel variations and completely bypass all current considered privacy preserving mechanisms.

IV. Applicability to Current Hardware

With our SDR-based testbed [9], [20][1] we are able to investigate how different vendors implemented the pseudo random seeding of the scrambler. An SDR consists of a hardware part that samples the electromagnetic spectrum and a software part that processes the samples and decodes the frames. For the hardware part we use the N210 from Ettus Research. For the software part we based our implementation on GNU Radio, a real-time signal processing framework.

Since IEEE 802.11p networks are not deployed, there are no commercial consumer systems available yet. Instead, experimentation is done with either very expensive prototype systems or adapted WiFi cards. We use our receiver to investigate the scrambler of IEEE 802.11p devices of either category.

First, we examine the Cohda Wireless MK2[2], a well-known prototype system, which has been used for major field trials in the US and in Europe. Besides Denso and NEC, Cohda Wireless is one of the leading suppliers of IEEE 802.11p prototypes. The MK2 is an ARM based PC with an IEEE 802.11p radio implemented on a Field Programmable Gate Array (FPGA) that ships with all the firmware and software of a complete IEEE WAVE enabled On-Board Unit (OBU) or RSU; we used firmware revision 4.0.14615.

As the second device, we investigate the Unex DCMA-86P2[3] miniPCI card, which has been used in the Grand Cooperative Driving Challenge. This card is based on the Atheros AR5413 WiFi chip. With Atheros being one of the market leaders for WiFi cards, this can be regarded as very representative Commercial Off The Shelf (COTS) hardware. The card is supported by the standard Linux kernel; we used the Linux 3.9.0 kernel with a modified ath5k driver that allowed us to set the bandwidth to 10 MHz and to tune to the DSRC/WAVE frequencies in the 5.9 GHz band.

We found that both devices implement a very simple – and most notably, a fully deterministic – algorithm to seed the scrambler. Our experiments revealed that the MK2 has a freewheeling scrambler in the sense that the state is not reset at all, but is running from frame to frame without reinitializing its state (as a side effect, this also means that if the packet size is a multiple of the cycle length of the scrambler, the seed does not change at all). The Unex card uses a simple counter, i.e., the initial scrambler seed is incremented by one for each frame that is sent. We tested different scenarios (e.g., we set the card to monitor and ad hoc mode, we generated cross-traffic that the card overheard) to make sure that no external parameter has an impact on either of the scramblers investigated.

Obviously, both algorithms allow for a trivial re-identification of consecutive frames from one card and, thus, to re-identify vehicles, even if MAC addresses (or pseudonyms) are changed between two frames. Since we assumed that also WiFi cards use over simplistic algorithms, we conducted initial experiments with COTS devices like a MacBook Air and indeed found suspicious behavior like network beacons with constant initial scrambler seed. An in-depth investigation of WiFi devices is, however, out of the scope of this paper and left for future work.

V. Implications on Privacy

The standards' definition of the scrambler is problematic in terms of privacy as it does not clearly state how the pseudo random sequence should be derived. From a communication performance perspective it is sufficient to change the scrambler values on a per-frame basis. This seems to have led to the situation that most vendors employ very simple algorithms, not considering possible implications on location privacy.

The most important privacy protection in vehicular networks is the use of pseudonyms that are changed according to some pseudonym changing strategy. To ensure location privacy and untraceability, messages sent by the same vehicle but with different pseudonyms must not be linkable to each other. If an eavesdropping attacker is able to use transmitted scrambler values to link messages regardless of their pseudonymous identifier, this privacy measure is circumvented and rendered useless. For example, in the case of a Unex card, which increments the scrambler value by one per frame, an attacker overhearing frames $\binom{A}{10}, \binom{A}{11}, \binom{B}{12}, \binom{B}{13}$, with $\binom{P}{n}$ being a frame with pseudonym P and scrambler state n, is (with all but certainty) able to identify A and B as being the same entity.

Also in more complex scenarios where an attacker put up several receivers but is not able to fully overhear all network traffic, non-random scrambler values can be used to still link messages with different pseudonyms. If the attacker is able to guess the amount of messages sent by a vehicle when it was not within the transmission range it can predict the scrambler values and then re-identify the vehicle. This attack becomes especially feasible when vehicles use static (or a discrete set of) beaconing frequencies, and in the case of Cohda devices, use messages of the same length.

VI. Evaluation of Impact

To obtain a quantitative indication of the impact of our attack on the location privacy of drivers in vehicular networks, we conducted an extensive set of simulations using the Veins

[1] http://www.ccs-labs.org/projects/wime/
[2] http://www.cohdawireless.com/
[3] http://www.unex.com.tw/product/dcma-86p2/

framework [21]. We extended the framework so that vehicles either used a simulated IEEE 802.11p radio from Cohda, Unex, or one that uses correctly implemented pseudo random scrambler values.

A. Simulation Setup

To be able to accurately gauge the impact of the scrambler attack, we investigate two challenging scenarios. Instead of the usual straight, fully covered stretch of freeway, we investigate a large urban intersection where vehicles can turn (Figure 2a) as well as a 3 km stretch of 3-lane freeway with a large blind spot (Figure 2b). We generated vehicular mobility in both scenarios using the microscopic traffic simulator SUMO and kept the number of vehicles constant throughout the simulation: for every vehicle that left the scenario a new one of a random preset type with a new, random route was inserted.

As we believe that the scrambler attack is able to circumvent privacy protection on the MAC layer and higher layers, such as pseudonym changes, we investigated a best case scenario for privacy: vehicles used a new pseudonym for each message, making it impossible to map messages based on any upper layer identifier. Also, vehicles emitted beacons with a frequency of only 1 Hz – the lowest possible beacon frequency according to the ETSI family of standards [22] – which represents the best case in terms of location privacy. The physical layer was simulated using two-ray-interference path-loss with a transmission power of 20 mW, leading to a theoretical transmission range of about 600 m. All parameters are summarized in Table I.

B. Attacker Model

The attacker in our simulation deployed (connected) receivers along the road and uses information such as the speed and the position, from the periodic broadcasts of vehicles. We furthermore assume that the attacker knows that different vendors use characteristic scrambler algorithms.

In the intersection scenario (cf. Figure 2a) the theoretical transmission range allowed the attacker to receive packets from vehicles approaching and leaving the intersection and on the intersection itself. A vehicle is considered tracked when it was possible to fully recreate the distinct path of a vehicle over the intersection from receiving the first packet until receiving the last packet. Note, as in our simulation the attacker is not omniscient but uses a radio receiver, he can experience packet loss and therefore lose track of a vehicle or associate an overheard beacon with the wrong vehicle.

Table I
SIMULATION PARAMETERS

Parameter	Setting
Framework	extended Veins
Scenarios	Intersection, Freeway
PHY/MAC	IEEE 802.11p/IEEE 1609.4
Transmission Power	20 mW
Radio Sensitivity	−89 dBm
Beacon Frequency	1 Hz
Simulation Time	300 s
Repetitions	50

In the freeway scenario (cf. Figure 2b), the attacker was not able to fully cover the whole scenario but placed two receivers along the freeway with a blind spot of 800 m between them. Here, a vehicle is considered tracked if it was possible to track its path from entering the transmission range of the first receiver and leaving the transmission range of the second one.

To perform the actual tracking we deployed an enhanced correlation tracking algorithm: When trying to associate received beacons with existing vehicle tracks, it accounted for physical limits of vehicular movement in terms of acceleration, speed, and heading and consecutively used Edmond's maximum weighted matching algorithm [23] to find the best association hypothesis. This tracking method is computationally inexpensive and has been shown to be very effective [24].

To understand the impact of the scrambler attack we compared this already advanced tracking algorithm with a variation that also exploited information about scrambler states: For each sequence of consecutively received beacons that the tracking algorithm deemed likely to be from the same vehicle (e.g., due to correlation of position, speed, etc.), it tried to infer which IEEE 802.11p device the vehicle might be using (by correlating the beacons' scrambler states). For vehicles where this succeeded, the tracking algorithm was then able to extrapolate future scrambler states and use this information to rule out potential associations of beacons and vehicles, limiting the number of candidate tuples and thus easing tracking.

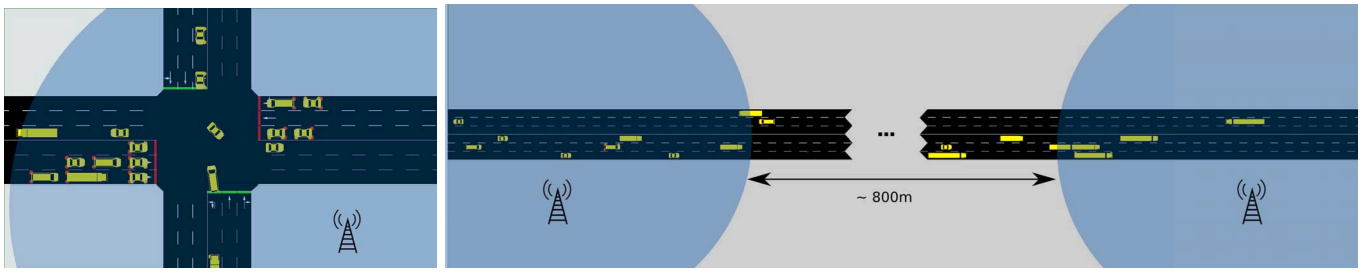
No other information was used for both tracking mechanisms. For example, the attacker did not exploit the beacon delay to determine which vehicle sent which beacon, as this could be easily prevented by distributing beacon events uniformly over the beacon period.

C. Results

Figure 3a shows our results for the intersection scenario. It shows the somewhat worrisome picture that it is almost impossible to confuse an attacker with pseudonym changes when (almost) all messages can be overheard. This confirms earlier findings [25], suggesting that in these cases privacy can only be achieved by not sending any packets. Although the tracking probability was already above 98 %, the usage of additional scrambler information could increase these values even more.

The results for the freeway scenario are shown in Figure 3b. The blind spot between the two receivers made it considerably harder (red line, square markers) for the attacker to track vehicles. Dynamics in the mobility of vehicles such as lane changing, overtaking, or varying velocities lead to wrong associations of beacons to vehicles on the attacker side. We observed that the mobility generated by SUMO seemed to be more dynamic as one would expect; to confuse a 'normal tracking' attacker in real life, the gap between the receivers would likely have to be wider. Congestion setting in at the highest vehicle density caused a slight increase in tracking probability, due to fewer lane changes and passing maneuvers.

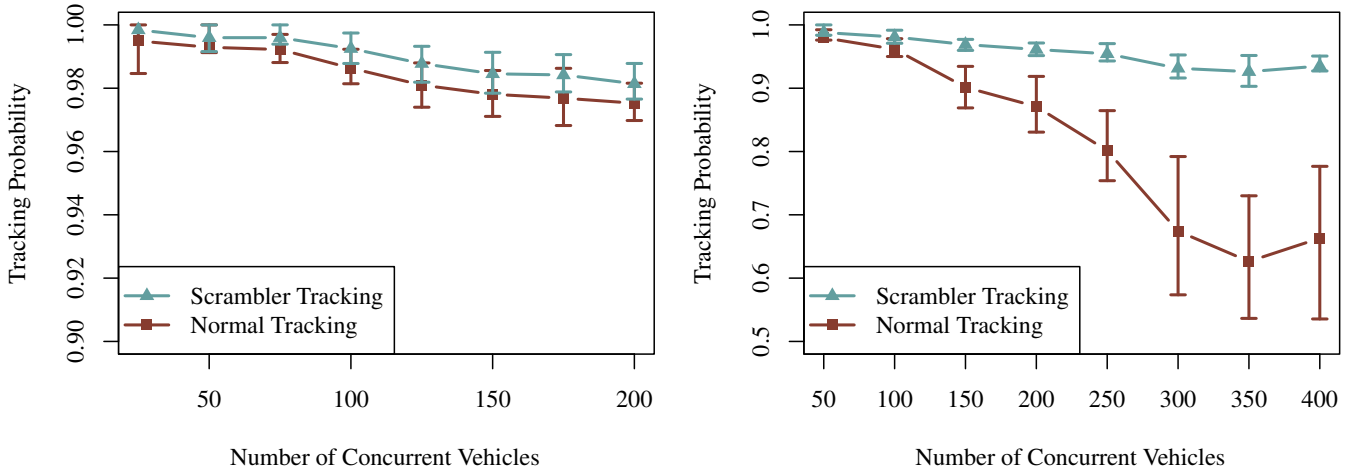
When the attacker used additional scrambler information to track vehicles the situation completely changed (teal line,



(a) Fully covered crossing scenario

(b) Freeway scenario with blind spot in between attacker receivers

Figure 2. Simulation Scenarios



(a) Intersection Scenario

(b) Freeway Gap Scenario

Figure 3. Impact of the Scrambler Attack in different scenarios

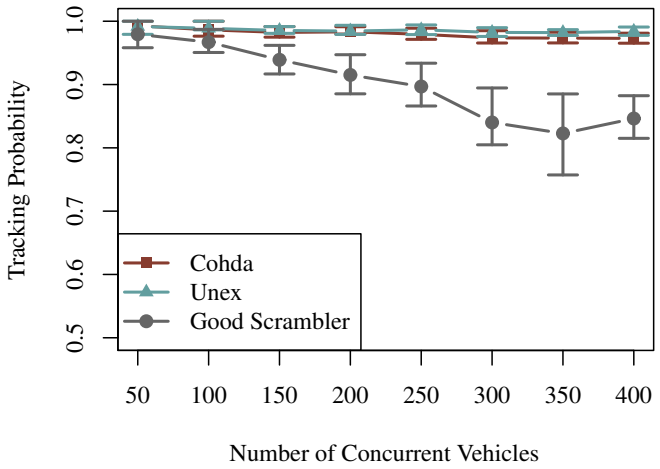


Figure 4. Tracking Probability depending on the type of IEEE 802.11p radio using the Scrambler Tracking Method

triangle markers): We observe that the gap between the two receivers only marginally influenced the capability to track vehicles. Approximating the number of beacons presumably sent by a vehicle while driving in the uncovered section of the freeway, the attacker is able to guess a number of possible scrambler values. Using this technique, we obtained tracking probabilities of over 95 %, almost reaching the level of the fully covered intersection scenario. This shows that even on a very busy freeway with interrupted radio coverage the scrambler attack allowed the attacker to effectively circumvent any higher layer privacy protection and track a large portion of vehicles. From this we conclude that also random silent times [26] (a privacy measure that is likely to be used in the final system [27]) can be rendered ineffective by non-random scramblers.

To fully illustrate the crucial requirement of unpredictable scrambler values we analyzed the results for the freeway scenario deeper, showing the tracking probability differentiated by the type of IEEE 802.11p radio (Figure 4). As can be seen, location privacy cannot be achieved using a predictable scrambler – the attacker was able to track almost every vehicle using the Cohda or the Unex radio. Even the vehicles using a random scrambler (gray line, circle markers) suffer from the now smaller number of vehicles possibly confusing an attacker. Their probability of being tracked is considerably higher than it was when scrambler values were not exploited to obtain information (Figure 3b, red line, square markers). This again underlines the necessity to address this problem and not allow for a circumvention of higher layer privacy measures.

VII. Countermeasures

The most obvious solution is to employ a cryptographic pseudo random number generator, possibly seeded by the large number of entropy sources in a vehicle (e.g., time when the vehicle was started, sensor values like fuel level and tire pressure, or meta data of communication like noise level, number of neighbors, and received data). Another solution is the deployment of constant network-wide scrambler values, however, this could possibly degrade network communication performance [19].

For the Cohda prototype platform this is straightforward since it does not rely on a transceiver chip but implements all logic on reconfigurable FPGAs. Therefore, it should be possible to fix the scrambling algorithm with a firmware update of the prototype.

For COTS hardware, the picture is different. Because vendors do not provide detailed information about their hardware design, it is hard to tell where certain functionalities are implemented and if this solution can be achieved with a driver or firmware update. In the worst case, the scrambling algorithm is implemented in hardware and hence cannot be fixed, but instead the chip would have to be changed.

VIII. Conclusion

We identified a novel attack vector on the location privacy of vehicles that leverages and exploits over-simplistic implementations of the pseudo random number generators used by an integral component of all WiFi and IEEE 802.11p radio transceivers. This component is the scrambler, which is crucial to ensure good performance at the physical layer. Sequences of the scrambler state can be predicted by overhearing a single packet, making it possible for an eavesdropper to associate different pseudonymous messages with the same sender. This passive, undetectable attack can be considered a physical layer attack; therefore no higher layer privacy mechanism such as the use of pseudonyms can compensate for it. In contrast to existing lower layer attacks, however, it is extremely robust, as it makes use of data rather than signal characteristics.

To show how severely location privacy can be degraded by our attack, we conducted an extensive set of simulations. Even in scenarios where vehicles traveled through sections where an adversary was not able to overhear messages, it was possible to reliably track vehicles. The results highlight the importance to use cryptographic PRNGs, not to increase the performance of the system, but to preserve the location privacy of drivers. We see our results as a first step towards enabling privacy protection mechanisms on a large scale.

References

[1] F. Dressler, H. Hartenstein, O. Altintas, and O. K. Tonguz, "Inter-Vehicle Communication - Quo Vadis," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 170–177, Jun. 2014.

[2] S. Rezaei, R. Sengupta, H. Krishnan, and X. Guan, "Reducing the communication required by DSRC-based vehicle safety systems," in *IEEE Intelligent Transportation Systems Conference (ITSC 2007)*. Seattle, WA: IEEE, Oct. 2007, pp. 361–366.

[3] F. Malandrino, C. Casetti, C.-F. Chiasserini, and M. Fiore, "Content downloading in vehicular networks: What really matters," in *30th IEEE Conference on Computer Communications (INFOCOM 2011), Mini-Conference*. Shanghai, China: IEEE, Apr. 2011, pp. 426–430.

[4] A. Vinel, "3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?" *Wireless Communications Letters*, vol. 1, no. 2, pp. 125–128, Apr. 2012.

[5] D. Eckhoff and C. Sommer, "Driving for Big Data? Privacy Concerns in Vehicular Networking," *IEEE Security and Privacy*, vol. 12, no. 1, pp. 77–79, Feb. 2014.

[6] M. Gruteser and B. Hoh, "On the Anonymity of Periodic Location Samples," in *Security in Pervasive Computing*. Boppard, Germany: Springer, Apr. 2005, pp. 179–192.

[7] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE, Tech. Rep. 1609.2, Apr. 2013.

[8] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," ETSI, TS 102 941 V1.1.1, Jun. 2012.

[9] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "Towards an Open Source IEEE 802.11p Stack: A Full SDR-based Transceiver in GNURadio," in *5th IEEE Vehicular Networking Conference (VNC 2013)*. Boston, MA: IEEE, Dec. 2013, pp. 143–149.

[10] B. Danev, D. Zanetti, and S. Čapkun, "On Physical-Layer Identification of Wireless Devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1–28, Nov. 2012.

[11] N. Patwari and S. K. Kasera, "Robust Location Distinction Using Temporal Link Signatures," in *13th ACM International Conference on Mobile Computing and Networking (MobiCom 2007)*. Montréal, Québec, Canada: ACM, Sep. 2007, pp. 111–122.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *13th ACM International Conference on Mobile Computing and Networking (MobiCom 2008)*. San Francisco, CA: ACM, Sep. 2008, pp. 116–127.

[13] M. Edman and B. Yener, "Active Attacks Against Modulation-based Radiometric Identification," Rensselaer Polytechnic Institute, Department of Computer Science, Tech. Rep. 09-02, Aug. 2009.

[14] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 544–555, Dec. 2009.

[15] O. Ureten and N. Serinken, "Wireless Security Through RF Fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, Winter 2007.

[16] T. Kohno, A. Broido, and K. Claffy, "Remote Physical Device Fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, May 2005.

[17] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. V. Randwyk, and D. Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," in *15th USENIX Security Symposium*. Vancouver, BC, Canada: USENIX, Jul. 2006, pp. 167–178.

[18] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, Std 802.11-2012, 2012.

[19] D.-W. Lim, S.-J. Heo, and J.-S. No, "An Overview of Peak-to-Average Power Ratio Reduction Schemes for OFDM Signals," *Journal of Communications and Networks*, vol. 11, no. 3, pp. 229–239, Jun. 2009.

[20] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An IEEE 802.11a/g/p OFDM Receiver for GNU Radio," in *ACM SIGCOMM 2013, 2nd ACM SIGCOMM Workshop of Software Radio Implementation Forum (SRIF 2013)*. Hong Kong, China: ACM, Aug. 2013, pp. 9–16.

[21] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[22] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI, EN 302 637-2 V1.3.0, Aug. 2013.

[23] J. Edmonds, "Maximum Matching and a Polyhedron with 0, l-vertices," *J. Res. Bur. Stand*, vol. 69B, no. 1-2, pp. 125–130, Jan. 1965.

[24] S. Blackrnan and R. Popoli, *Design and Analysis of Modern Tracking Systems*. Artech House Boston, 1999.

[25] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough," in *7th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2010)*, Kranjska Gora, Slovenia, Feb. 2010.

[26] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, New Orleans, LA, Mar. 2005.

[27] SAE Int., "Dedicated Short Range Communications (DSRC) Message Set Dictionary," SAE, Tech. Rep. J2735-200911, Nov. 2009.