Wireless Channel-Based Message Authentication

Ala'a Al-Momani and Frank Kargl
Institute of Distributed Systems
Ulm University, Germany
Email: alaa.al-momani@uni-ulm.de
Email: frank.kargl@uni-ulm.de

Christian Waldschmidt
Institute of Microwave Techniques
Ulm University, Germany
Email: christian.waldschmidt@uni-ulm.de

Steffen Moser and Frank Slomka
Institute of Embedded Systems/
Real-Time Systems
Ulm University, Germany
Email: steffen.moser@uni-ulm.de
Email: frank.slomka@uni-ulm.de

***Abstract*—Inter-vehicle communication has attracted a lot of attention in the past. A major concern is the security and especially the integrity and authenticity of messages. Current standards and proposals in literature leverage asymmetric cryptographic mechanisms to achieve this, which is costly both in terms of consumed computational power, bandwidth, and introduced delay. We present a novel idea to use physical characteristics of the wireless channel to verify subsequent messages after initial trust in a first message has been established cryptographically. In this paper, we sketch the concept and provide a first evaluation on its potential for saving named resources.**

I. Introduction

Looking at security in communication systems, lower layers of the communication system security and especially the physical layer are often disregarded for solutions. Security is introduced and implemented by means of cryptographic mechanisms only on the network layer and above. This comes at a significant overhead which results from complex cryptographic calculations and the need for additional security payload to be integrated into packets. With this paper, we want to propose an alternative approach that relies on physical-layer channel characteristics for message authentication in Car-to-X (C2X) communication.

One of the basic functionalities of envisioned C2X systems is a periodic transmission of broadcast messages (so-called beacons [1], [2]) in order to inform others about the sender's position, speed, heading and similar information.

In order for the receiver to distinguish whether the beacon originated from a legitimate vehicle, an approach based on ECDSA-based digital signatures and a public key infrastructure is currently proposed [3], where each vehicle is equipped with an asymmetric key pair and a digital certificate where the public key is amended with a number of attributes (e.g., lifetime, vehicle type, license plate number) and signed by the certification authority [4], [5], [6]. The secret key is used to sign all outgoing messages. The resulting signature, as well as the sender's certificate are attached to each message. Receivers first check the signature for correctness and then check the certificate. If both are valid, receivers will accept messages, otherwise they are discarded.

This way, one can distinguish messages sent by valid vehicles from arbitrary messages that were, e.g., generated and sent by attackers using a laptop on the roadside.

Unfortunately, verifying the signature on the receiver side is time and resource consuming [7], which increases the delay of signaling a warning to the driver and requires more computing power. In addition, digital signatures increase the packet size significantly, leading to more collisions on the potentially already congested channel. The considerable execution time in creating or verifying signatures could be solved using more powerful CPUs or Hardware Secure Modules (HSMs) [6]. A drawback of these solutions is that they incur additional and significant cost.

In this paper, we propose the idea of a novel and unorthodox approach for *re*-authenticating periodic messages like cooperative awareness messages (CAMs) without these drawbacks. Leveraging the unique physical properties of the wireless channel between a specific sender and receiver, we want to base authentication of subsequent packets on these characteristics once an initial packet has been authenticated cryptographically.

We also provide a preliminary "back-of-a-napkin" estimate of our scheme's effectiveness and resource savings, which we aim to refine and verify in future research.

II. Wireless Channel-Based Message Authentication

A. Authentication in IEEE 1609.2 or ETSI 103 097

The authentication process as proposed in standards like IEEE 1609.2 [3] or ETSI 103 097 [8] foresees that senders generate digital signatures on packets to be sent and attach these signatures together with an optional certificate to messages. The receiver then has to verify each received certificate. The Elliptic Curve Digital Signature Algorithm (ECDSA) [9], with the NISTp256 curve was chosen as cryptographic underpinning.

This whole procedure increases transmission delay, requires computational resources and increases packet size and thus chance for collisions of packets on the wireless channel. Many researchers have pointed this out in the past [4], and some [10] even suggest to skip some of the security processing for the sake of performance on a fraction of packets.

For some time, researchers on wireless security have been considering exploiting characteristics of the radio channel to design security mechanisms that are more lightweight. This includes mechanisms that derive cryptographic keys [11], [12]

978-1-4673-9411-6/15/$31.00 ©2015 IEEE

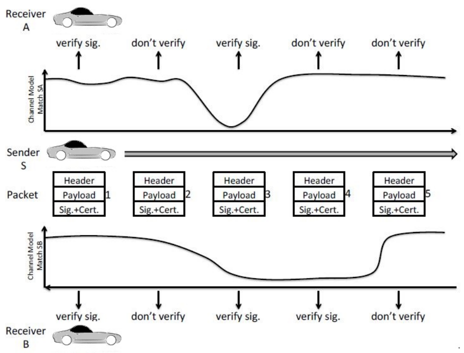

Fig. 1. Wireless Channel Based Message Authentication.

or those which try to "fingerprint" a specific radio-module in order to re-authenticate it in future encounters [13].

B. The proposed Scheme

We take a slightly different approach. Our new approach considers (re)authentication of earlier communication partners by characteristics of the communication channel. It is based on the observation that a radio channel between transmitter and receiver has a unique signature (for example defined by multi-path propagation, Doppler shifts...), which is hard for an attacker to guess or manipulate as long as the attacker covers a different position in space than sender or receiver.

If it is possible to measure this channel signature and if the channel signature is stable beyond messages–or we can predict it a short time into the future–, periodic data packets could be authenticated based on this channel signature. For this purpose, a first beacon would be authenticated by means of classical cryptography, establishing an initial trust anchor.

As long as the channel remains sufficiently stable between this and a consecutive packet, all subsequent packets could now be authenticated by the means of their channel signature associated with the original transmitter. Costly cryptographic verification processes may potentially be skipped altogether for some packets.

The process is exemplified in Figure 1. A transmitter S sends periodic messages. The first message has to be cryptographically verified in any case in order to produce an initial trust anchor. Thereafter, messages are only verified cryptographically if the receiver trust at A or B in the packet being delivered over the same channel falls below a certain threshold. For receiver A, the third message needs to be cryptographically verified while messages 3 and 4 need to be verified for receiver B case.

Figure 2 shows a more detailed example. The signature of packet 1 has to be cryptographically verified by the receiver; leading to a trust level of 100% in this packet. For packet 1, the receiver will also measure channel characteristics as a baseline for the following packet. For the subsequent packet 2, the same channel characteristics will be measured leading to a confidence of 90% that the channel was indeed the same. Likewise For packet 3, the receiver determines with 70% confidence level that the packet was sent over the same channel as packet 2. Assuming that both measurements are independent, we can calculate an overall trust level of 63% that the sender of the third packet is the same as the first packet sender which was cryptographically verified. This approach, shown in Figure 2, is our basic scheme for wireless channel-based message authentication. It assumes a linear dependency between sequential packets.

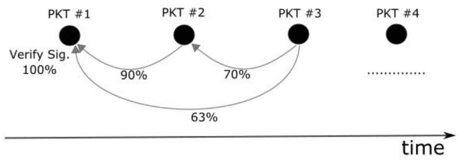

Fig. 2. The proposed scheme.

There can be different variations of this method. One could be assuming a Bayesian probability between the sequential packets from one sender, and the probability that the last received packet comes from the first sender given the dependency probability between sequential packets. Other probabilistic models which could be used here are Markov Chains or hidden Markov models. This is going to be explored in our future research.

C. Channel Characteristics

For our scheme to work, we need to identify suitable characteristics of the channel between the sender and the receiver to identify the sender based on them without checking the signature. Requirements for these characteristics include:

- Measurable: receivers need to be able to observe and measure the specific characteristics
- Stable: the specific characteristics need to be sufficiently stable and reliable beyond a number of packets so that they can serve to conclude that two packets are actually related.
- Unspoofable: attackers should not be able to spoof the characteristics, luring receivers into accepting false packets.

We are currently evaluating various of these characteristics with respect to their suitability to serve for wireless channel-based message authentication. As part of this, we are looking into different parameters which can potentially be gathered from the physical layer:

- Average power of received signal
- Doppler spread
- Delay spread and distribution caused by multi-path propagation
- Short- and long-term channel state information (CSI) or channel impulse response (CIR)
- Exploiting beam forming systems to gather directivity information of a signal.

All of these can be measured with more or less effort in modern receiver architectures proposed for C2X. Stability is more of a concern as our scheme requires that the communication channel is relatively stable and somehow predictable at least on short term. This is a challenging requirement in vehicular networks in general due to the fact of the rapid movement of vehicles. On the other hand, high periodicity of messages from a sender of up to 10 Hz will shrink the time between any two messages so that this may still be applicable. Considering multi-path propagation, a noteworthy feature in this regard is the distribution of received voltage at the receiver side, which follows Rice distribution. Depending on the ratio of the deterministic (LOS) component and the statistical multi-path components, the distribution becomes a Gauss distribution in the presence of a dominant deterministic component. However, it becomes a Rayleigh distribution in the absence of this component.

Whether spoofing is possible requires deeper analysis. In general, one can assume that attackers will not be able to predict channels as their characteristics are so volatile. However, knowing positions of sender and receiver may still allow the attacker to estimate, e.g., the average Signal-Noise-Ratio.

D. Extracting Channel State Information

We suppose that using the channel state information or the impulse response will provide us with the most significant information about the channel environment. Not all types of receivers which are currently planned for use in C2X communication measure and calculate this parameter. This has to be kept in mind, as it is the goal of our approach to reduce the overall computational load of the C2X nodes by reducing the amount of cryptographic signature checks. The introduction of additional tasks in signal processing–like the retrieval of channel information–has to be considered as a trade-off and might undermine any performance gain.

In the last years some research work has been focusing on improvements of the PHY layer in C2X systems compared to a plain single-input/single-output (SISO) IEEE 802.11p receiver. For example, multi-antenna systems using beam forming to direct transmission power into a specific area have been proposed [14], [15]. Also systems exploiting recent advances in single-user or multi-user multiple-input/multiple-output (MIMO) communication systems have been proposed and studied [16], [17], [18], [19]. MIMO systems using Orthogonal Space-Time Block Codes (OSTBC) similar to IEEE 802.11n or IEEE 802.11ac, can be used to extend the spectral efficiency of the communication system. This can be used in two ways by making the communication more robust or by increasing the data rate. Both aspects can be very interesting for C2X communication when it comes to reliable communication or to overcome congested channels. The PHY layer in MIMO systems typically needs to have the ability to estimate the channel state information (CSI) based on pilot tones at least on the receiver's side. This information is required to separate the received data streams into parallel channels.

Such information will be an interesting starting point to evaluate our approach together with advanced PHY approaches like single-user or even multi-user MIMO systems which will deliver the information we need intrinsically.

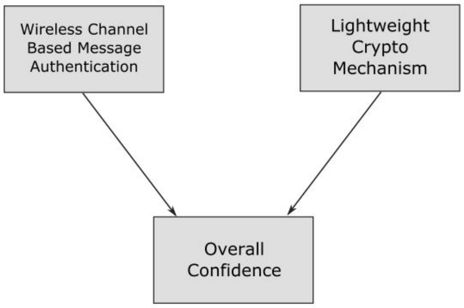
Wireless Channel Based Message Authentication
Lightweight Crypto Mechanism
Overall Confidence

Fig. 3. The Enhanced Scheme.

E. System Requirements

We propose this scheme for C2X communication, as C2X shows some characteristics that make it very suitable for our approach. We note that wireless channel-based message authentication may also be suitable for other domains if the requirements described in this section are fulfilled.

Generally, our scheme requires periodic transmission of packets at a frequency that is high enough – in compliance with the standards – to have multiple packets sent by one sender before channel changes too significantly. Furthermore, it is specifically suited for communication systems that have broadcast communication among unpredictable sets of senders. Our system also works if communication partners are stable and known in advance. However, in this case, message authentication solutions based on symmetric cryptography may be better suited as one can more easily agree on session keys.

III. SCHEME VARIANTS

In the previous discussion we presented only the most basic variant of our scheme. However, we also foresee many possible enhancements.

One issue may be that the overall confidence that any packet sender is the same as the first packet sender drops down quickly below a value where you can rely on it to accept packets. This would mean that receivers have to resort to verifying signatures in order to re-establish cryptographic trust again, reducing the efficiency of our scheme significantly.

As a solution, we could use multi-factor authentication by combining the proposed scheme with another lightweight cryptography scheme to enhance the authentication as shown in Figure 3. This can be achieved by adding another light-weight signature with very short key length in addition to the ECDSA signature. So if the confidence level of wireless channel-based authentication drops below a threshold, one could in addition verify the light-weight signature in order to increase the level of confidence while light-weight signatures alone could be easily cracked by an attacker.

A second enhancement that we foresee makes use of a prediction of movement mechanism [20], considering privacy aspects, in order to better estimate the channel characteristic based on the new position of the sender. Information from C2X CAM messages can help in predicting new positions and also know important information like speed, heading, etc...

On the other hand, the proposed approach could be integrated into misbehaviour detection frameworks [21] foreseen for C2X systems such like position falsification detection in VANETs. For example, if an attacker claims to be at position X' while he is at position X and the obtained information from the channel characteristics state that he is impossible to be at the position X', then this can help to detect attacks.

IV. SUMMARY AND FUTURE WORK

The proposed scheme promises to reduce security overhead in C2X communication systems. At the same time, we face substantial challenges before being able to finally implement and evaluate such schemes.

One challenge lies in time-variant scenarios such as communicating through unstable channel conditions due to the rapid movement of participants. Here we are currently investigating multiple channel characteristics and their stability in C2X communication scenarios using simulations. To include signal processing in C2X simulations, we can rely on an integrated software-defined radio approach described in [22]. This allows us to study channel characteristics, signal processing and network behaviour in a holistic simulation framework based on VEINS/OmNeT++. We also foresee practical experiments with IEEE 802.11p networks.

Additional questions that we need to address include: Is it possible for an attacker to spoof the channel to mislead the receiver? How could the trust probabilities be developed? How can the light weight crypto mechanism be designed? How could their decisions be combined together? How can we measure and evaluate the security level gained by our scheme?

Designing and evaluating the proposed scheme and answering above questions require in-depth investigation and cooperation between experts in IT security and experts in wireless communication which is one of the goals of our research.

REFERENCES

[1] ETSI, "Intelligent transport systems; vehicular communications; geonetworking; basic set of applications; part 2: Specification of cooperative awareness basic service." vol. Technical Specification: TS 102 637-2, no. V1.1.1., 2011.

[2] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*. IEEE, 2007, pp. 1–6.

[3] IEEE, "Trial-use standard for wireless access in vehicular environments - security services for applications and management messages," no. IEEE Std 1609.2-2006, 2006.

[4] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005, pp. 11–21.

[5] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung *et al.*, "Secure vehicular communication systems: implementation, performance, and research challenges," *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 110–118, 2008.

[6] P. Papadimitratos, L. Buttyan, T. S. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 100–109, 2008.

[7] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "Sevecom-secure vehicle communication," in *IST Mobile and Wireless Communication Summit*, no. LCA-POSTER-2008-005, 2006.

[8] T. ETSI, "103 097: Intelligent transport systems (its)."

[9] ANSI, "Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm," no. ANSI X9.62, 1998.

[10] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in *Proceedings of the third ACM conference on Wireless network security*. ACM, 2010, pp. 111–116.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 128–139.

[12] A. Loch, D. Meier, and M. Hollick, "How did you get here? phy-layer path signatures," in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*. IEEE, 2014, pp. 1–3.

[13] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security*. ACM, 2010, pp. 89–98.

[14] S. Moser, S. Eckert, and F. Slomka, "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks," in *Proceedings of the International Conference on Future Generation Communication Technology (FGCT)*, London, UK, Dec 2012, pp. 36–41.

[15] H. Stuebing, A. Jaeger, N. Wagner, and S. A. Huss, "Integrating Secure Beamforming into Car-to-X Architectures," *SAE International Journal of Passenger Cars- Electronic and Electrical Systems*, vol. 4., pp. 88–96, Jun. 2011.

[16] K. Sundaresan, R. Sivakumar, M. A. Ingram, and T.-Y. Chang, "Medium Access Control in Ad Hoc Networks with MIMO Links: Optimization Considerations and Algorithms," *Mobile Computing, IEEE Transactions on*, vol. 3, no. 4, pp. 350–365, 2004.

[17] N. F. Abdullah, A. Doufexi, and R. J. Piechocki, "Spatial Diversity for IEEE 802.11p Post-Crash Message Dissemination in a Highway Environment," in *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*. IEEE, 2010, pp. 1–5.

[18] A. El-Keyi, T. ElBatt, F. Bai, and C. Saraydar, "Mimo vanets: Research challenges and opportunities," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, Jan 2012, pp. 670–676.

[19] S. Moser, L. Behrendt, and F. Slomka, "MIMO-enabling PHY Layer Enhancement for Vehicular Ad-Hoc Networks," in *Proceedings of Wireless Communications and Networking Conference Workshops (WCNCW), 2015, IEEE*, New Orleans/LA, USA, March 2015, pp. 142–147.

[20] H. Stübing, A. Jaeger, N. Bißmeyer, C. Schmidt, and S. A. Huss, "Verifying mobility data under privacy considerations in car-to-x communication," in *17th ITS World Congress*, 2010.

[21] R. van der Heijden, S. Dietzel, and F. Kargl, "Misbehavior Detection in Vehicular Ad-hoc Networks," in *1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013)*, Innsbruck, Austria, February 2013.

[22] D. Maier, S. Moser, and F. Slomka, "Deterministic Models of the Physical Layer through Signal Simulation," in *Proceedings of the Eighth International Conference on Simulation Tools and Techniques (SIMUTOOLS)*, Athens, Greece, August 2015.