View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Dokumenten-Publikationsserver der Humboldt-Universität zu Berlin

Physical Layer-Based Message Authentication in VANETs

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

Frank Kargl
Institute of Distributed Systems
Ulm University, Germany
Email: frank.kargl@uni-ulm.de

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

***Abstract*—Authenticating legitimate nodes is a major concern of the envisioned vehicular networks. To achieve this, standards and literature propose to use asymmetric cryptographic mechanisms which generate significant overheads in terms of time and power consumption. In this paper, we address this problem and we propose a novel idea of exploiting physical layer characteristics to rely on them for re-authenticating future beacons after verifying the first one cryptographically. Despite the challenges in such high mobility networks, possible concrete approaches to start the evaluation of our scheme are presented. Our approaches are inspired by the vehicular channel related work conclusions which give signs of future success to our scheme in this critical field.**

I. INTRODUCTION

As pointed out in [1], in contradiction with other networks, securing vehicular networks at the physical layer has been disregarded. The reason of this is the nature of such networks by means of the high mobility of vehicles, which makes investigating physical layer and exploiting its information for the sake of security a challenging task. In standards, the foreseen authentication process states that digital signatures in addition to certificates have to be generated and attached to messages by senders. The digital signatures are based on Elliptic Curve Digital Signature Algorithm (ECDSA) [2] where each vehicle is equipped with a public and a secret key; the secret key is used to sign all outgoing messages while the public key is amended with some other attributes forming the certificate of the vehicle. Receivers then check signatures and certificates of messages for correctness and decide whether they are originated from legitimate senders or would-be intruders, e.g. roadside attackers.

In order to inform neighbouring vehicles about the current state, vehicles have to keep sending their states periodically with a frequency of 1-10 Hz including the position, the speed, the heading and other similar information in messages called "beacons". For each beacon, the procedure for generating and attaching signatures needs to be executed at the sender side. In addition, receivers have to keep verifying newly received beacons even if they are from the same sender. This whole procedure to ensure that only legitimate vehicles are able to exchange messages among each others in the network creates significant overheads due to the complex cryptographic calculations resulting in major drawbacks that should be highlighted. The following gives a summary of these shortcomings::

- The decrease of bandwidth utilization due to the increase in message size that is necessary because of the must-included signature.
- The increase in packet collisions due to the increase of the number of packets per message in an already congested channel.
- The increase in the end-to-end delay because of:
  - The increase in the required time to generate signatures.
  - The increase of the transmission delay due to the need for transmitting additional bits.
  - The increase in the required time due to the verification process of signatures at the receivers.

In this paper, we restrict our concerns to the last issue that points out the long time needed to verify the ECDSA-based signatures. We propose the idea of a novel scheme for re-authenticating the periodic messages, i.e. beacons, in vehicular networks. By exploiting the unique physical layer features between a specific sender and a specific receiver, we aim to eliminate the drawbacks of the classical authentication mechanisms proposed in the standards of vehicular networks while maintaining a reasonable degree of security.

We also provide concrete approaches to start the evaluation of our scheme inspired by the outcome from propagation studies in realistic vehicular environments which gives signs of success to our proposed scheme. Moreover, we propose the idea of multi-factor authentication with the use of subjective-logic [3].

II. RELATED WORK

The previous authentication process takes place in the upper layers of the OSI model. Researchers have realized its drawbacks and pointed them out, for example, [4; 5]. In order to mitigate them, some researchers [5] suggested to use hardware secure modules, but equipping vehicles with sophisticated processing units adds additional cost. Others suggested to omit signatures and certificates to reduce the introduced latency in order to achieve reasonable efficiency for the critical applications [6], but this will lead to insecure networks where unauthenticated nodes are able to spoof and inject messages into networks.

A. Security at the Physical Layer

The previous shortcomings in the upper layers′ security motivate researchers in other wireless communication networks to look for other solutions. They suggested to integrate the physical layer into the authentication process in static and low mobility networks [7; 8; 9; 10; 11; 12].

Mainly, the work in exploiting physical layer features for the use of security and authentication can be divided into two classes:

- Class 1: Extracting the secret key from the common wireless channel between the transmitter and the receiver, e.g. [9; 10; 11].
- Class 2: Fingerprinting the wireless channel established between the transmitter and the receiver, e.g. [7; 8; 12].

Both of them are based on the fact that the wireless channel established between a specific transmitter and a specific receiver is unique and only known to both of them. The first class uses the unique channel variation to establish the secret key. This approach is considered secured such that only the transmitter and the receiver are able to construct the key. However, the verification process still has to be applied in this case, which means that the long verification time still exists. On the other hand, the second class does not require any key extraction or verification. It relies on the uniqueness of the frequency response for each transmitter-receiver pair, and hence a receiver identifies a transmitter based on the history it has for that transmitter. This way, the need of the signature verification process vanishes with its drawbacks while maintaining a reasonable degree of security.

At 5 GHz, over a span o 10 MHz, with indoor stationary user terminals, Xiao et al. [7; 8] proposed ways to exploit spatial variability of the frequency response. They found that variations are strongly correlated in time while very weakly correlated in space giving a positive impact on performance in such a static scenario. In addition, they concluded that channel time variations can improve performance whereas frequency correlation degrades it. Their results show that it is possible to distinguish between legitimate nodes and other illegitimate nodes based on the corresponding physical layer characteristics to each one of them.

B. Vehicular Channel Propagation Models

The distinct features of vehicular networks arise from the nature of the rapidly changing topology due to vehicles′ rapid movement. This results in a significant uniqueness in the statistical characteristics of the multipath propagation in V2V communication compared to other indoor or even cellular communication. The investigation of vehicular channel characterization is fairly young research topic [13]. It gained researchers′ interest when WAVE initiative and other vehicular applications raised concerns regarding vehicular communication. Before 2006, V2V channel characteristics were rarely investigated, e.g. [14] [15]. Since 2006, there has been a lot of research, e.g. [16; 17; 18; 19; 20; 21; 22; 23; 24], addressing the vehicular channel propagation models based on measurement campaigns considering different frequency bands.

One of the earlier works on V2V channel investigation at the 5.9 GHz band is [25], where the Tapped Delay Line (TDL) approach was used to model the channel. They stated that these kind of channels are doubly selective, in other words, they are both time- and frequency-selective channels. Also at 5.9 GHz, Cheng et al. [21] conducted a measurement study on V2V narrow-band channel; they presented a single- and dual-slope large-scale path loss model with Nakagami distribution to describe the small-scale fading. In addition, they introduced the Speed-Separation (S-S) diagram, which is a new tool for understanding and estimating Doppler spread and coherence time.. Kunisch and Pamp did a measurement experiment in [24] at 5.9 GHz over a span of 20 MHz, in which they extracted the scattering function which contains information about Doppler spread and path delays. They also provided a good explanation of each propagation path scenario.

Other measurement studies were conducted at different bands. In [16], Karedal et al. were able to track individual propagation paths at 5.2 GHz. Paier et al. [17] investigated pathloss, Power Delay Profiles (PDPs), and Delay-Doppler spectra from a highway measurement over 240 MHz at 5.2GHz where the transmitter and the receiver vehicles travelled in opposite direction. Examples of other studies at different bands are [26] at 5.3 GHz, and [27] at 5.6 GHz.

III. Physical Layer-Based Message Authentication

A. Requirements

For our scheme to work, physical layer characteristics have to meet some requirements in order to be able to rely on them for future verification of beacons without checking the signatures. Requirements for these characteristics include:

- Stability: The characteristics should show stability over at least two consecutive beacons. In other words, the time correlation of this specific physical layer characteristic should be high enough to ensure its stability within the reception of two consecutive beacons.
- Uniqueness: to allow discrimination among several transmitters in the vehicular network, the uniqueness of the physical layer characteristic among them has to be ensured. This means that the characteristic the receiver relies on has to be spatially uncorrelated to be able to distinguish between several transmitters at different locations at the same time. However, due to vehicles movement, this characteristic should allow a degree of spatial correlation such that the measured value of the characteristic when vehicle A at location X is correlated with the measured value when the same vehicle is at location X'. A noteworthy point in this regard is that vehicles do not move in random paths, but in deterministic tracks where prediction of movement could be easily employed.
- Measurable: receivers need to be able to observe and measure the specific characteristics.
- Unspoofable: attackers should not be able to spoof the characteristics, luring receivers into accepting false messages.

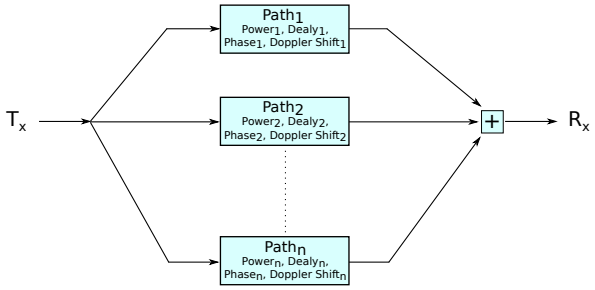

Fig. 1. Multipath Model

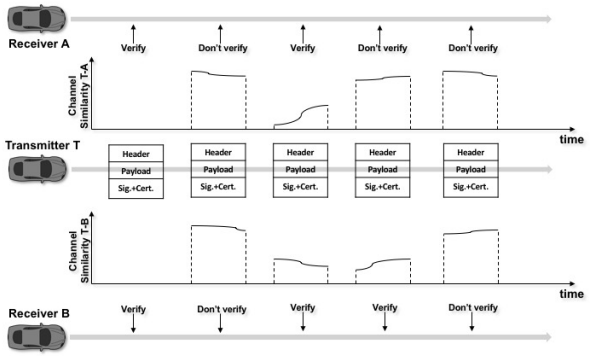

Fig. 2. Physical Layer Based Message Authentication

B. The Proposed Scheme

We take a slightly different approach than the classical fingerprint approach discussed earlier. 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 characteristic with a unique signature (for example defined by multi-path propagation, Doppler shifts...), which is hard for an attacker to guess or manipulate. Hence, instead of looking at the frequency response, as it may be challenging in high mobility scenarios, looking at the individual multipath components and extracting their characteristics will provide more robustness. Such a case is shown in Figure 1 where each contribution has its own delay, power, phase, and Doppler shift.

The conducted measurement studies showed that each average PDP consists of several identifiable contributions and that they are presented over several consecutive time instants (typically in order of seconds) [27]. This was the observation in [26] and [16] as well. Hence, periodic beacons 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 charachteristic remains sufficiently stable between this and a consecutive beacon, all subsequent beacons could now be authenticated by the means of their channel signature associated with the original transmitter. Costly cryptographic verification processes may potentially be skipped for some beacons.

The process is exemplified in Figure 2. A transmitter T 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 message being delivered over the same channel falls below a certain threshold. Receiver A needs to cryptographically verify the third beacon while beacons 3 and 4 need to be verified for receiver B′s case.

C. Multi-factor Authentication and Possible Enhancement

Multi-factor Authentication can play a role in the authentication process where the receiver can rely on different observations to form his opinion about the received beacon whether it is originated from a legitimate node or not. In order to avoid resorting to the cryptographic verification to rebuild the overall confidence in the latter beacons, the receiver may combine the output from our proposed scheme with another lightweight authentication mechanism. This requires a sufficient degree of flexibility of the outputs to be combined together and allow multi-factor authentication process. Hence, we here foresee the use of subjective logic to form a holistic framework for such authentication mechanisms where each factor (e.g. multipath characteristics, lightweight authentication mechanism, etc...) gives an opinion about the received beacon whether it is generated from the same transmitter as the previously received beacons or not. Subjective logic extends the classical logic theory by introducing a degree of certainty to each opinion. It has a wide set of operators allowing the fusion of individual factor opinions into one opinion taking the degree of certainty of each output into account. It has been deployed in VANETs in [28] to form a misbehaviour detection framework which our proposed scheme could be integrated into.

IV. CONCLUSION

This paper addresses the shortcomings of using ECDSA-based signatures in the envisioned V2V communication to achieve a proper authentication of the periodic beacons. The main drawback of such signatures is the long verification time needed to verify the signature by the receiver. We proposed a novel idea of integrating physical layer into the authentication process aiming at eliminating the shortcomings of the upper layer authentication mechanisms. Inspired by related work in vehicular channel propagation models outcome, which gives signs of future success for our scheme, we proposed concrete approaches to start the evaluation of the proposed scheme, in addition to proposing possible ways of enhancements including multi-factor authentication using subjective logic.

REFERENCES

[1] A. Al-Momani, F. Kargl, C. Waldschmidt, S. Moser, and F. Slomka, "Wireless channel-based message authentication," in *Vehicular Networking Conference (VNC), 2015 IEEE*. IEEE, 2015, pp. 271–274.

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

[3] A. Josang, "Artificial reasoning with subjective logic," in *the second australian workshop on Commonsense Reasoning*, vol. 48, 1997, p. 34.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[5] 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.

[6] 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.

[7] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 7, pp. 2571–2579, 2008.

[8] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Communications, 2007. ICC'07. IEEE International Conference on*. IEEE, 2007, pp. 4646–4651.

[9] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 321–332.

[10] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 205–215, 2011.

[11] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[12] I. O. Kennedy and A. M. Kuzminskiy, "Rf fingerprint detection in a wireless multipath channel," in *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on*. IEEE, 2010, pp. 820–823.

[13] C. F. Mecklenbraüker, A. F. Molisch, J. Karedal, F. Tufvesson, A. Paier, L. Bernadó, T. Zemen, O. Klemp, and N. Czink, "Vehicular channel characterization and its implications for wireless system design and performance," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1189–1212, 2011.

[14] A. S. Akki and F. Haber, "A statistical model of mobile-to-mobile land communication channel," *Vehicular Technology, IEEE Transactions on*, vol. 35, no. 1, pp. 2–7, 1986.

[15] J. Maurer, T. Fugen, and W. Wiesbeck, "Narrow-band measurement and analysis of the inter-vehicle transmission channel at 5.2 ghz," in *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, vol. 3. IEEE, 2002, pp. 1274–1278.

[16] J. Karedal, F. Tufvesson, N. Czink, A. Paier, C. Dumard, T. Zemen, C. F. Mecklenbräuker, and A. F. Molisch, "A geometry-based stochastic mimo model for vehicle-to-vehicle communications," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 7, pp. 3646–3657, 2009.

[17] A. Paier, J. Karedal, N. Czink, C. Dumard, T. Zemen, F. Tufvesson, A. F. Molisch, and C. F. Mecklenbräuker, "Characterization of vehicle-to-vehicle radio channels from measurements at 5.2 ghz," *Wireless personal communications*, vol. 50, no. 1, pp. 19–32, 2009.

[18] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, "Experimental study on the impact of vehicular obstructions in vanets," in *Vehicular Networking Conference (VNC), 2010 IEEE*. IEEE, 2010, pp. 338–345.

[19] S. A. H. Tabatabaei, M. Fleury, N. N. Qadri, and M. Ghanbari, "Improving propagation modeling in urban environments for vehicular ad hoc networks," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 12, no. 3, pp. 705–716, 2011.

[20] Y. Jeong, J. W. Chong, H. Shin, and M. Z. Win, "Intervehicle communication: Cox-fox modeling," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 418–433, 2013.

[21] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1501–1516, 2007.

[22] N. Akhtar, S. C. Ergen, and O. Ozkasap, "Vehicle mobility and communication channel models for realistic and efficient highway vanet simulation," *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 1, pp. 248–262, 2015.

[23] I. Sen and D. W. Matolak, "Vehicle–vehicle channel models for the 5-ghz band," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 9, no. 2, pp. 235–245, 2008.

[24] J. Kunisch and J. Pamp, "Wideband car-to-car radio channel measurements and model at 5.9 ghz," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*. IEEE, 2008, pp. 1–5.

[25] G. Acosta-Marum and M. Ingram, "Doubly selective vehicle-to-vehicle channel measurements and modeling at 5.9 ghz," in *Proc. Int. Symp. Wireless Personal Multimedia Commun*. Citeseer, 2006.

[26] O. Renaudin, V.-M. Kolmonen, P. Vainikainen, and C. Oestges, "Wideband mimo car-to-car radio channel measurements at 5.3 ghz," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*. IEEE, 2008, pp. 1–5.

[27] J. Karedal, F. Tufvesson, T. Abbas, O. Klemp, A. Paier, L. Bernadó, and A. F. Molisch, "Radio channel measurements at street intersections for vehicle-to-vehicle safety applications," in *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*. IEEE, 2010, pp. 1–5.

[28] 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.