FADEC: Fast Authentication for Dynamic Electric Vehicle Charging

Hongyang Li
University of Illinois Urbana-Champaign
hli52@illinois.edu

György Dán
KTH Royal Institute of Technology
gyuri@kth.se

Klara Nahrstedt
University of Illinois Urbana-Champaign
klara@illinois.edu

I. Introduction

Dynamic wireless charging [1], [2] is a promising technology for charging electric vehicles (EV) while driving. The basic idea is to place charging coils under the charging pads on the road and attach charging coils to the EV's battery. When the EV is driving above the coil, the electromagnetic interaction between the coils under the road and the coils in the EV can charge the EV battery.

Dynamic charging is only possible with proper communication support. Before charging starts, the EV should inform the charging pads several its battery type, current state-of-charge, desired charge rate, etc. The utility may also send price schedule frames to the EV if real-time pricing is employed. During the charging session, the EV periodically reports its charging status to the utility, which uses the reports to detect abnormal charging behavior, and to build a real-time charging profile. When the charging session ends, the EV also exchanges messages with the utility to confirm the total received energy for billing purpose.

A natural candidate for EV to utility communication is the Dedicated Short Range Communication (DSRC), where roadside units (RSUs) along the road help relay messages between EVs and the utility. Clearly, EVs would have to authenticate with the RSUs to ensure they send their reports to the right RSU. At the same time, the RSUs would have to authenticate messages received from the EVs to implement access control. Signing messages and verifying signatures must be fast, since the RSUs would have to handle the authentication of reports from many EVs. The authentication mechanism also needs to support mobility, because an EV could communicate with the utility company through different RSUs as it moves along a road.

The IEEE 802.11p standard suggests the use of Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication in vehicular networks. Recent work [3] has shown, however, that ECDSA could take a significant amount of time to sign a message and to verify a signature, which makes it susceptible to DoS attacks. To overcome the disadvantage of computation overhead of ECDSA, researchers have proposed the use of one-time signature for authentication [3]–[6]. However, one-time signature is not the ideal solution in our scenario since it could incur non-trivial key generation and signing overhead [4], requires delayed verification [5], or puts restrictions on the content to be authenticated [3].

This material is based upon work supported by the Department of Energy under Award Number DEOE0000097. The views expressed are the responsibility of the authors and do not represent the views of the funding agency.

We propose *Fast Authentication for Dynamic EV Charging (FADEC)* to support the communication needs of dynamic wireless EV charging. FADEC features fast message signing, fast signature verification, fast hand-off authentication, and low communication overhead. FADEC allows the EV to use the same key to authenticate with a series of RSUs, so that the EV does not have to re-authenticate itself every time it encounters a new RSU.

II. FADEC System Design

We consider a scenario where EVs periodically send battery status reports to the utility. EVs send their reports to RSUs through DSRC, and the RSUs relay the reports to the utility through backbone connection. An EV e could establish a session key K_e^u with the utility and use HMAC to authenticate its communication with the utility. However, since all messages between EV e and the utility are relayed by RSUs, the communication between the EV e and the RSUs must also be authenticated. FADEC achieves this by first establishing a session key K_e^r with the RSU currently associated with the EV e, which allows the use of HMAC authentication for EV-RSU communication.

Once the key K_e^r between EV e and the current RSU is established, our goal is to allow EV e to communicate with all the subsequent RSUs using K_e^r. FADEC follows a broadcast-and-discard approach for key dissemination, as illustrated in Fig. 1. When RSU A first establishes key K_e^r with EV e, it broadcasts the key to all its neighbor RSUs (in terms of proximity along the road) through the backbone network. When a neighbor RSU B receives K_e^r, it stores the key for $t_{A\to B}$ seconds, where $t_{A\to B}$ is a fixed parameter that estimates the maximum time required for an EV currently in range of RSU A to move into the range of B. If EV e does not try to communicate with RSU B using K_e^r within $t_{A\to B}$ time then RSU B discards the key. Similarly, when C receives K_e^r, it stores the key for $t_{A\to C}$ seconds. In Fig. 1, EV e is moving towards C, and enters the range of C within $t_{A\to C}$ seconds. If EV e communicates with RSU C using K_e^r, then C will broadcast K_e^r to its neighbor RSUs, and will itself store the key for additional t_C seconds, where t_C is a fixed parameter

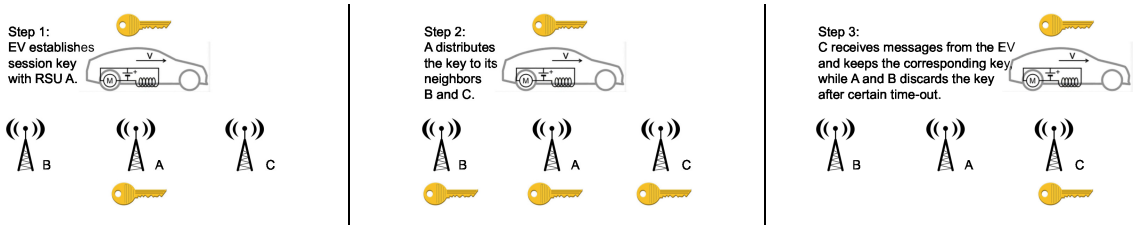

Fig. 1. Illustration of key establishment, dissemination to neighbors and discarding of unused keys.

estimating the duration when EV e stays within the range of C. Note that only the RSU currently associated with the EV will broadcast K_e^r to its neighbor RSUs. This prevents flooding and helps keep the RSU key storage small. Our simulations confirm that in a heavily loaded highway scenario each RSU needs to hold about 30 keys on average.

Compared with the conventional approach [7] for key distribution in VANET which predicts the next RSU that the EV will encounter and send the key only to that RSU, the FADEC approach has two major advantages: (i) FADEC does not need to predict the individual mobility of each EV. For example, when there are multiple roads between RSU A and B, FADEC can use the road that takes the longest time to travel to estimate $t_{A\to B}$. (ii) FADEC can tolerate high inaccuracy in the estimated value of $t_{A\to B}$ and t_B because, as long as the estimated values are sufficiently large, an inaccurate estimation will not cause the RSU to discard the key prematurely and thus there is no need to re-establish session keys. In the conventional mobility-prediction approach [7], if the EV does not move towards the predicted next RSU, it has to run the key exchange protocol again to establish a new session key with the RSU, which could consume several seconds of valuable contact time with the RSU.

In practice, RSU B could estimate the value of $t_{A\to B}$ as

$$t_{A\to B} = \frac{d_{A\to B}^{max}}{v_{A\to B}^{min}} \tag{1}$$

where $d_{A\to B}^{max}$ is the maximum travel distance to enter range of B from range of A, and $v_{A\to B}^{min}$ is the minimum speed of an EV. $d_{A\to B}^{max}$ can be calculated from the road map, and $v_{A\to B}^{min}$ can either be estimated from past traffic statistics, or can take the value of minimum speed limit in highway scenario. The RSU may also use different values of $d_{A\to B}^{max}$ and $v_{A\to B}^{min}$ at different time of day to accommodate varying traffic speed and density and achieve better estimation. t_B can be estimated in a similar fashion.

III. Performance Evaluation

We simulate road traffic on a 4-lane single-direction straight road segment of 3km with 5 RSUs along the road. We generate mobility traces from a congested traffic flow with 7284 EV/hour and maximum vehicle speed of 75 km/h. The backbone propagation delay between the utility and each RSU is 100 ms, and the delay between neighbor RSUs is set to 10 ms. We evaluate FADEC in two scenarios with different assumptions on the computational resource available to the EV and the RSU. In the *resource rich* scenario, we assume the EV and the RSU have a strong CPU to sign messages and to verify signatures, where signing and verifying a digital signature both take 20 ms; whereas in the *resource constrained* scenario, digitally signing a message and verifying a digital signature both take 200 ms. In both scenarios each EV periodically sends a 1024-bit report to the utility, and each report must be delivered within 5 seconds.

Using FADEC, most EVs are able to achieve a delivery ratio close to 1 in both scenarios. Using ECDSA results in lower delivery ratios, especially in the resource constrained scenario, where only 57% reports are delivered successfully on average. Our simulation also shows that FADEC achieves almost the same delay with an average of 0.117 second in both scenarios. On the other hand, the average delay of ECDSA in the resource rich scenario is 0.180 second, and increases to 4.805 seconds in the resource constrained scenario. In the resource constrained scenario, the time to sign a message and to verify a signature using ECDSA significantly increases. This greatly affects the delay of ECDSA.

IV. Conclusion and Future Work

In this paper we have presented FADEC, authentication for dynamic electric vehicle charging. FADEC lets EVs establish symmetric keys with the RSUs and the utility company, and achieves fast signing, fast verification, fast hand-off authentication, and low communication overhead. Our simulations have shown that FADEC obtains very close to 1 report delivery ratio and small delay in both resource rich and constrained scenarios. Compared with ECDSA, FADEC reduces the data delivery delay by at most 97% and improves the delivery ratio by more than an order of magnitude. In the future we will perform a thorough security analysis of FADEC, as well as evaluate its performance under more complex traffic scenarios.

References

[1] "Stanford report," http://news.stanford.edu/news/2012/february/wireless-vehicle-charge-020112.html.

[2] X. Yu, S. Sandhu, S. Beiker, R. Sassoon, and S. Fan, "Wireless energy transfer with the presence of metallic planes," *Applied Physics Letters*, vol. 99, no. 21, 2011.

[3] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient broadcast authentication for vanets," in *MobiCom*, 2011.

[4] L. Reyzin and N. Reyzin, "Better than biba: Short one-time signatures with fast signing and verifying," in *ACISP*, 2002.

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *IEEE SP*, 2000.

[6] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM*, 2009.

[7] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *Wireless Communications, IEEE*, vol. 16, no. 4, pp. 16–22, 2009.