2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems

An Authentication Framework for Electric Vehicle-to-Electric Vehicle Charging Applications

Braden Roberts*, Kemal Akkaya†, Eyuphan Bulut‡ and Mithat Kisacikoglu§
*Dept. of Comp. Science, Southern Utah University, Cedar City, UT 84720, Email: bradenroberts@suumail.net
†Dept. of Elec. and Comp. Engineering, Florida International University, Miami, FL 33174, Email: kakkaya@fiu.edu
‡Dept. of Comp. Science, Virginia Commonwealth University, Richmond, VA 23284, Email: ebulut@vcu.edu
§Dept. of Elec. and Comp. Engineering, University of Alabama, Tuscaloosa, AL 35487, Email: mkisacik@ua.edu

***Abstract*—Electric vehicles are becoming parts of our daily lives with the increasing investment from auto industry. However, their charging is an issue as this requires frequent charging and longer waiting times compared to traditional gasoline-based vehicles. The charging is typically done at residential or public charging stations. With the increased dominance of electric vehicles, one potential solution is to exploit vehicle-to-vehicle charging (V2V) where an electric vehicle can charge another one through a converter-cable assembly. In such cases, however, there needs to be a protocol between the charge supplier and receiver to authenticate each other and authorize the vehicle to open its charging ports. In this paper, we study this problem of authentication and propose a protocol that will utilize key exchange among the users without relying on certificates. We implemented the proposed protocols under Wi-Fi Direct and Bluetooth and demonstrated that the approach can provide the necessary framework of communication before charging starts without any additional overhead.**

***Index Terms*—V2V charging; Authentication; Electric vehicles; Diffie-Hellman key exchange**

I. Introduction

Plug-in electric vehicles (EVs) have been receiving increasing popularity to reduce the dependency on fossil fuels and promote adoption of intermittent renewable energy sources by acting as energy storage systems [1]–[4] during the periods of strong wind or sun [5]–[7]. EVs can also help in realizing the foundation of smart cities of the future by injecting energy to the grid during periods of reduced production to balance demand. Due to such potential, many automotive companies have already begun to roll out EVs from their production lines [8]–[10]. As an example, by 2020 California will need about 13 to 25 times the roughly 8,000 work and public chargers it currently has, to support the need for EVs. Currently, about 23,000 public charging stations have already been deployed in the US and it is expected that there will be fast-charging stations built on major highways.

One of the major challenges of EV deployment has been large-scale infrastructure investment to support EV growth. Such mass charging of EVs will not only require a very high budget but also put a lot of stress on the power grid [11], [12]. In particular, significant degradation of power system performance can arise under high penetration levels of uncoordinated charging [13], [14]. However, this is not the only problem as the EVs require long-periods of frequent charging as opposed to fossil-driven vehicles. For instance even Tesla's Supercharger stations can charge a car in about 30 minutes, more than twice as fast as the standard fast charger, which is still a long time compared to gas filling. With such a charge, the average travel distance is around 100 miles that creates the problem known as *range anxiety* for the drivers. Thus, the charging needs to be scheduled in advance depending on the route of the EVs. This necessitates large number of charging stations distributed throughout the cities, particularly, in the states like California, where the expected number of EVs will be one third of the total vehicles by 2024. In fact, the widespread adoption of EVs also depends on the availability of a large enough number of charging stations.

An ultimate solution that can quickly accelerate EV adoption rates lies in the ubiquity of vehicle-to-vehicle (V2V) energy transfer. Specifically, through the cooperation and interaction of EV owners in local communities with an appropriate communication infrastructure, EVs can share their energy and mitigate the aforementioned problems [15]. The main motivation for this solution comes from the application of the trending *sharing economy* framework [16], which has many successful examples such as AirBNB [17], and Uber [18]. Recently, there have been a growing interest from academia and industry on the application of energy transfer in mobile networks [19]–[21] including vehicular networks and several studies have been conducted analyzing different aspects (e.g., pricing [19], [22], [23], range anxiety [15]) of V2V energy exchanges.

To realize a V2V energy transfer, initially there should be a matching between the suppliers and receivers. Once the demander EVs make a query within their neighborhoods, the best supplier EVs that will satisfy the charging needs of demander EVs should be identified. This could be achieved via a centralized control and EV owners can use a dedicated app designed for them to connect and manage their participation. During the search process, an EV owner looking for charging can select a supplier EV among multiple alternatives and then make the payment through the online app (possibly, using third party services). However, when it comes to actual energy transfer, the demander EV and supplier EV need to physically meet and connect the their batteries through a specially designed dc-dc converter. That is, either the demander EV needs to drive to the location of the supplier EV or the supplier EV can come to the location of the demander EV, if the demander is willing

2155-6814/17 $31.00 © 2017 IEEE
DOI 10.1109/MASS.2017.93

to pay a service fee. In any case, the EVs need to authenticate each other to ensure that no other supplier/demander EV shows up and even if one of the owners is not there, the energy transfer is possible in the agreed amount.

In this paper, we study the authentication problem among the EVs that will exchange energy. To this end, we propose using a mutual challenge/response protocol (e.g., Mutual CHAP) [24] that will utilize DSRC communication among the EVs. In this protocol, both EVs will send a randomly generated challenge to each other, both in clear text and in hashed form using a shared secret K. The receiving part will regenerate the hashed form using the shared secret K and compare with the received one for authentication. Therefore, we also need to ensure that the EVs agree on a shared secret K. This K will be generated after the search process when two EV users agree on the energy sharing exchange (e.g., a confirmation is sent from the demander to the supplier that it was selected). We propose using a form of Diffie-Hellman (DH) key exchange [25] to agree on K. However, since DH is vulnerable to man-in-the-middle (MiTM) [26] attacks, both parties need to authenticate the process. The challenge here is to use DH without relying on certificates, as ordinary users may not rely on certificate authorities. For this purpose, both parties need to check the validity of the exchanged DH public parameters and report these DH parameters to each other and then perform a comparison of them visually or loudly over a communication channel. Since this is not practical, we will follow a protocol based on string comparison proposed in [27].

Once the key K is generated at both users' ends, the next step is to transfer this key to the EV's on-board DSRC unit. We propose using a Bluetooth-based communication to enable this process. A hashed value of the shared secret will be sent to the EV's DSRC unit with the time of charging and transaction ID of the EV-EV charging.

We make our implementations and experiments using Android phones. Our experiment results show that our proposed method can provide authentication of the EVs without relying on third parties. In the literature, there are various authentication schemes proposed for vehicular networks [28] that use hash and shared keys. Our proposed method differs from them as it does not rely on third parties for shared key management, instead a DH based key exchange mechanism is used.

The rest of the paper is organized as follows. We discuss our assumptions, problem definition and motivation in Section II. Section III gives details about our proposed MTD-based data report scheduling. In Section IV, performance evaluation is discussed. Finally, the paper is concluded in Section V.

II. Preliminaries

A. System Model and Assumptions

We assume a system model where the EVs carry on-board units (OBUs) to communicate with the upcoming DSRC standard and have a Controlled Area Network (CAN) bus linked to the charging port. These OBUs have interfaces to the vehicle's display unit or to the driver's smartphone via Bluetooth or Wi-Fi as seen in Fig. 1. Dedicated Short Range Communication (DSRC) standard allows EVs to talk to each other through their OBUs for safety purposes [29]. This standard is expected to be deployed on every vehicle after 2021. The smartphones are assumed to be owned by the EV owners, which will be used to exchange charging information and agree on price, location, time, etc. for charging. Note that smartphones can either communicate via a cellular infrastructure (e.g., LTE) or through DSRC-based infrastructure which can utilize the existing OBUs for multi-hop communication in case there is no cellular Internet access.

Fig. 1: Sample OBU that supports Wi-Fi, Bluetooth and DSRC standards.

B. Problem Statement

Our problem can be defined as follows: "An EV owner needs his/her vehicle charged and needs to authenticate another EV owner with a compatible charger that is able to charge his/her vehicle. The EV owners agree on a time frame for charging but in cases where the taker would like to get his/her EV charged without standing by his/her EV, the EVs should be able to automatically authenticate each other."

C. Attack model

In our scenario, we assume the following attack model:

The attacker sits in the middle of the EV owners (i.e., giver and taker) and can obtain/change the exchanged key for authentication. This can be performed by a man-in-the-middle (MiTM) attack. Another way to obtain this key is when it is sent to the EV through Wi-Fi or Bluetooth if it is not encrypted.

This key can then be used to authenticate the EVs. The attacker can then take charge from the EV rather than giving charge to that particular EV. In another scenario, the attacker may impersonate the taker and authenticate his/her car to take charge from the giver.

III. Proposed Protocol

In this section, we describe the proposed EV-EV charging coordination protocol in more details.

A. Overview

In our proposed suite of protocols that will enable coordination among the users, the vehicle owner or demander (D) and charger supplier (S) first agree on a time frame for which the vehicle will be ready and available for charging. After such agreement, D and S generate a secure key K using a version of Diffie-Helman (DH) key exchange over a peer-to-peer connection, such as LTE or Wi-Fi Direct. If the shared key is generated successfully, a unique transaction ID (ID_K) is produced and stored on each device. Note that the K has a certain lifetime based on the charging time. In the second step, the K is transmitted to OBUs of the involved vehicles by their respective owners. This transmission can be done either via Wi-Fi or Bluetooth again. Once the key is available on the OBUs and pre-scheduled time comes, the EVs authenticate each other and the charging ports are opened through CAN bus of the EV. The overall process is shown in Fig. 2.

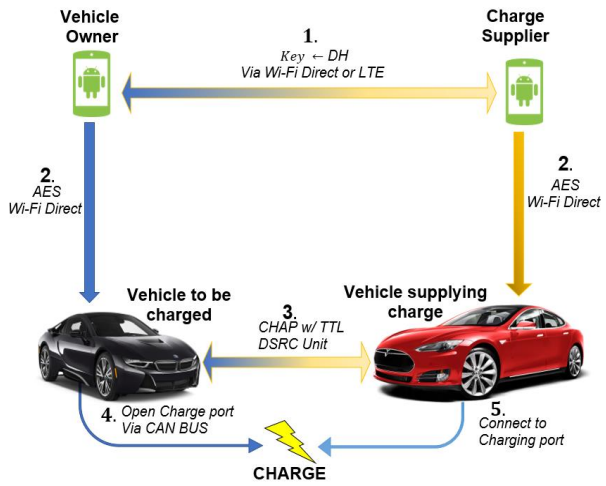

Fig. 2: Proposed V2V charging protocol, which provides secure charging between peer vehicles.

B. Diffie-Hellman Key Exchange Without Certificates

The Diffie-Hellman key agreement protocol [25] is a commonly used protocol that provides security against eavesdroppers. We describe the basic protocol as follows. Two users, A and B, need to agree on a shared key and have public shared key g and prime modulus n. A proceeds to generate a secret key X_A and calculates $g^{X_A} \ mod \ n$. B also generates a secret key X_B and calculates $g^{X_B} \ mod \ n$. A and B exchange these calculated values and compute the shared secret key $(g^{X_B})^{X_A} \ mod \ n$ and $(g^{X_A})^{X_B} \ mod \ n$ respectively. Both A and B generate the same key without revealing their individual private keys.

It is well known that the basic version of DH is susceptible to a man-in-the-middle (MiTM) attack from an active adversary. The attacker simply needs to generate his own DH parameters and broadcast it to A and B. In [27], they were able to redirect traffic between two legal parties through an attacker. To prevent this type of an attack, there are versions of DH which add authentication to both parties. However, this authentication is typically done by relying on certificates that should be owned by the users. This means, an ordinary user with a charging app needs to also obtain his/her own certificate and store in his/her phone so that DH can be securely implemented when two parties communicate. As this is a cumbersome task which may not be pursued by ordinary users, we opted for another solution which will not rely on certificates as described below.

The Secure Key Exchange (SKE) protocol as introduced in [30], uses a commitment scheme which incorporates two important cryptographic principles: Once a sender commits to a specific value, it cannot be altered (*binding*) and a commitment cannot be used by the receiver until the sender opens it (*hiding*). In our implementation, we incorporated a commitment scheme using SHA-256 hashing. A sender wanting to send the message m transforms it into a commitment/opening pair of the form $(c, d) \leftarrow commit(m)$, where $c = sha\text{-}256(m)$ and $d = m$. Thus when the sender is ready to commit m, he hashes it and sends that value to the receiver. When the sender is ready to open m, he simply sends d to the receiver who verifies it in the form $m \leftarrow open(c, d)$ by taking the SHA-256 hash of d and comparing it with c, if the values are equal then $d = m$. If the sender were to alter m in any way after sending c, then the hashes would not match thus the commitment is binding. The value c by itself does not reveal any information about m therefore the commitment is also hiding.

Prior to SKE, two users, A and B agree on public keys g and prime modulus n. A and B then generate a human readable identifier ID_A and ID_B, a private key X_A and X_B as well as a random k-bit binary string N_A and N_B. A and B then form $m_A = ID_A||g^{X_A}||N_A$ and $m_B = ID_B||g^{X_B}||N_B$ using concatenation. A then uses the commitment scheme as described above to compute $(c, d) \leftarrow commit(m_A)$. A sends c to B who responds by sending m_B. At this point, A sends d to B who opens $m_A \leftarrow open(c, d)$. The final stage of the protocol begins with A and B computing $S_A = N_A \bigoplus N'_B$ and $S_B = N_B \bigoplus N'_A$, where N'_B and N'_A are the messages received. A and B send S_A and S_B to each other and then visually verify if they match. If they match, A generates $K = (g^{X_B})^{X_A} \ mod \ n$ and B generates $K = (g^{X_A})^{X_B} \ mod \ n$.

C. Proposed EV-EV Mutual Authentication

After key generation, the next step is to ensure that this key is sent to the EVs' OBUs so that when they come closer to each other they can mutually authenticate each other. Specifically, D and S send K, ID_K and time to live (TTL) information to their vehicle, V_D and V_S respectively. TTL value is crucial here since after the charging takes place, the

key will no longer be valid. The key transfer is secured using AES Encryption and occurs over a peer-to-peer (P2P)-based network such as Wi-Fi Direct or Bluetooth. It is important to note that this step needs to occur prior to S arriving to authenticate with V_D.

When S arrives to charge V_D, a mutual challenge handshake authentication protocol (CHAP) is used to authenticate both parties using the DSRC unit of each vehicle. Both V_S and V_D generate a random number challenge, C_S and C_D respectively, and send it to each other. V_D computes $H_D \leftarrow hash(C'_S||K)$ and V_S computes $H_S \leftarrow hash(C'_D||K)$ with $hash$ representing the MD5 hash function and $'$ representing the received values. V_S and V_D transmit H_S and H_D respectively. V_S verifies $H'_D = hash(C_S||K)$ and V_D verifies $H'_S = hash(C_D||K)$ and if both parties verify then authentication succeeds. It is important to note that V_D is equipped with a time to live (TTL) protocol that erases K after the agreed time expires, thus V_S and V_D cannot authenticate outside of the agreed time frame.

If authentication is successful, V_D communicates via the OBU using the CAN bus to open up the charging port of the vehicle. At this point S connects his vehicle (V_S) to V_D and commences to charge. An example to the implementation of the V2V charging after the authentication is the CHAdeMO protocol that is used by Nissan, Toyota, etc [31]. Through CHAdeMO, the giver vehicle can initiate and control the charging power transfer process via communicating with the taker EV using CAN bus. According to this protocol, taker EV behaves as if it is connected to a fast charging station. The charging ends whenever the taker EV stops the process.

IV. Protocol Implementation and Testing

In this section, we provide the details of the experiments and discuss the experiment results.

A. Experiment Setup

We implemented this protocol using two Android devices and a computer with both Wi-Fi and Bluetooth capabilities. We programmed our Android application using Android Studio and installed it on a Google Nexus 4 and a Samsung Galaxy J320. We used the laptop to emulate the functionality of a DSRC unit for the vehicle to be charged. The laptop also contained a Virtual Machine (VM) containing the Linux distribution Ubuntu which had a Linux-CAN kernel installed to simulate the opening of the charging port.

The smartphones were paired using Wi-Fi direct and the DH protocol was initiated. We performed experiments using three DH based protocols.

- Basic DH which provides no mutual authentication.
- DH with String comparison (DH-SC) as described in [27].
- SKE protocol as described above.

We performed DH sharing in three different environments that would typically be seen when key agreement takes place: inside of a building, outside and building to outside.

To provide an optimum balance of security and usability we set $k = 55$ when testing DH-SC and SKE. In order to make this 55-bit string more readable, we encoded it into 5 words, each word containing 4 characters or less, using the predefined dictionary used in RFC 2289 [32]. Each phone displayed the 5 word string of both parties and the users verified the strings were identical.

Afterwards, the phone representing the demander paired with the laptop via Wi-Fi direct to transmit the key to the laptop using AES. Then the phone representing the supplier paired with the laptop via Bluetooth and mutual CHAP was initiated.

If successful, the laptop then sent a signal from Windows 10 to the VM to simulate the opening of the charging port via the Linux-CAN module.

B. Performance Metrics

In our simulations we used two performance metrics. These metrics are end-to-end delay and transmission range.

- The average *End-to-end (ETE) delay* for the DH protocols, excluding user mutual authentication.
- The average *Transmission Range* which indicates the transmission distance from a smart phone to a vehicle to be charged.

C. Performance Results

1) ETE Delay: Based upon our experiments, we observed that our ETE delay was smallest for the basic DH protocol. We calculated an average delay of 219 ms from the start of DH to key generation. Of the two DH protocols that used mutual authentication, SKE appeared to be faster with an average delay of 1036 ms. DH-SC had an average delay of 1405 ms. Our results showed that there was significantly ($p < 0.001$) less of a delay using the basic DH when compared to those that used mutual authentication. There was, however, no significance difference ($p > .05$) in the ETE delays between DH-SC and SKE.

2) Transmission Range: In terms of transmission range, we conducted experiments to assess the effective transmission range to understand the feasibility of usage from work/home to an EV. We observed a maximum range while outside, as we were able to achieve a consistent data transfer range of 35-40 meters with Wi-Fi Direct. The most expected scenario is communication from building to outside that produced a range of about 32 meters which is pretty much similar to outside performance. Finally, for outside transmission while inside a building (e.g., cases where the vehicle is parked in an underground garage and the work environment is within the same building) produced the smallest range of 22 meters with consistent data transfer.

D. Security Analysis

The proposed approach provides mutual authentication among the EVs which means that any impersonator will be failed to be authenticated. Consequently, any malicious person who would like to charge a different vehicle or take away charge from an existing vehicle will be prevented.

TABLE I: ETE Delay of DH protocols

	Basic DH	DH-SC	SKE
Delay(ms)	219	1405	1036

Regarding the shared key; this exchanged key will not be exposed to third parties. First, DH has been proven to be secure. There can be no integrity or impersonation attacks. Second, when the key is transmitted to the EV, it is encrypted and will not be known to unauthorized parties.

V. Conclusion

In this paper, we proposed a series of authentication protocols to be used for EV-to-EV charging applications. The main motivation is to prepare EVs to get charged through the use of existing standards such as DSRC, Wi-Fi Direct or Bluetooth. We employ a shared key exchange protocol that does not rely on certificates for authentication.

We implemented and tested the proposed protocols using smartphones and Wi-Fi Direct protocols. The experiments showed that the proposed framework can be adapted with existing standards that can be easily deployed in real-life. In the future, we plan to integrate the protocols with EV's CAN bus to open the charging port.

Acknowledgment

Braden Roberts in this work is supported by US National Science Foundation under the grant number REU-CNS-1461119.

References

[1] W. Kempton and A. Dhanju, "Electric vehicles with V2G," *Windtech international*, vol. 2, no. 2, p. 18, 2006.

[2] T. Markel, M. Kuss, and P. Denholm, "Communication and control of electric drive vehicles supporting renewables," in *Proc. of IEEE Vehicle Power and Propulsion Conference, VPPC'09*, 2009, pp. 27–34.

[3] C. Guille and G. Gross, "The integration of PHEV aggregations into a power system with wind resources," in *Proc. of Bulk Power System Dynamics and Control (iREP)*. IEEE, 2010, pp. 1–9.

[4] H. Lund and W. Kempton, "Integration of renewable energy into the transport and electricity sectors through V2G," *Energy policy*, vol. 36, no. 9, pp. 3578–3587, 2008.

[5] N. DeForest, J. Funk, A. Lorimer, B. Ur, I. Sidhu, P. Kaminsky, and B. Tenderich, "Impact of widespread electric vehicle adoption on the electrical utility business–threats and opportunities," *Center for Entrepreneurship and Technology (CET) Technical Brief*, no. 2009.5, 2009.

[6] S. M. Lukic, J. Cao, R. C. Bansal, F. Rodríguez, and A. Emadi, "Energy storage systems for automotive applications," *IEEE Transactions on Industrial Electronics*, vol. 55, no. 6, pp. 2258–2267, 2008.

[7] S. Lukic, "Charging ahead," *IEEE Industrial Electronics Magazine*, vol. 2, no. 4, pp. 22–31, 2008.

[8] Tesla Motors-High Performance Electric Vehicles, "Available online: http://www.teslamotors.com."

[9] Nissan LEAF Electric Car, "Available: http://www.nissanusa.com/leaf-electric-car."

[10] Chevrolet, "2011 volt electric car," *Available: http://www.chevrolet.com/electriccar*.

[11] W. Su and M.-Y. Chow, "Performance evaluation of an EDA-based large-scale plug-in hybrid electric vehicle charging algorithm," *Special Issues on Transportation Electrification and Vehicle-to-Grid Applications, IEEE Transactions on Smart Grid*, 2011.

[12] S. Shao, M. Pipattanasomporn, and S. Rahman, "Grid integration of electric vehicles and demand response with customer choice," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 543–550, March 2012.

[13] C. Roe, E. Farantatos, J. Meisel, A. Meliopoulos, and T. Overbye, "Power system level impacts of PHEVs," in *Proc. of Hawaii International Conference on System Sciences, HICSS'09*, Jan 2009, pp. 1–10.

[14] E. Sortomme, M. Hindi, S. MacPherson, and S. Venkata, "Coordinated charging of plug-in hybrid electric vehicles to minimize distribution system losses," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 198–205, March 2011.

[15] E. Bulut and M. Kisacikoglu, "Mitigating range anxiety via vehicle-to-vehicle social charging system," in *Proceedings of Vehicular Technology Conference (VTC Spring), IEEE*, 2017.

[16] PWC, "Consumer intelligence series: The sharing economy," April 2015. [Online]. Available: https://pwc.com/CISsharing

[17] "Airbnb." [Online]. Available: https://www.airbnb.com/

[18] "Uber." [Online]. Available: https://www.uber.com/

[19] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 8, no. 3, pp. 33–44, 2016.

[20] D. Niyato, P. Wang, D. I. Kim, W. Saad, and Z. Han, "Mobile energy sharing networks: Performance analysis and optimization," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3519–3535, 2016.

[21] E. Bulut and B. K. Szymanski, "Mobile energy sharing through power buddies," in *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*. IEEE, 2017, pp. 1–6.

[22] R. Zhang and X. Cheng, "Stable matching based cooperative v2v charging mechanism for electric vehicles," in *Proceedings of Vehicular Technology Conference (VTC Fall), IEEE*, 2017.

[23] M. Wang, M. Ismail, R. Zhang, X. S. Shen, E. Serpedin, and K. Qaraqe, "A semi-distributed v2v fast charging strategy based on price control," in *Global Communications Conference (GLOBECOM), 2014 IEEE*. IEEE, 2014, pp. 4550–4555.

[24] C. Latze, U. Ultes-Nitsche, and F. Baumgartner, "Strong mutual authentication in a user-friendly way in eap-tls," in *Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. 15th International Conference on*. IEEE, 2007, pp. 1–5.

[25] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[26] A. S. Khader and D. Lai, "Preventing man-in-the-middle attack in diffie-hellman key exchange protocol," in *Telecommunications (ICT), 2015 22nd International Conference on*. IEEE, 2015, pp. 204–208.

[27] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 467–478, 2006.

[28] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, 2017.

[29] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, A. Bucceri, and T. Zhang, "Vehicular communications using DSRC: challenges, enhancements, and evolution," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 399–408, 2013.

[30] W. Shen, W. Hong, X. Cao, B. Yin, D. Shila, and C. Yu, "Secure key establishment for device-to-device communications," in *Global Communications Conference (GLOBECOM), 2014*. IEEE, 2014, pp. 336–340.

[31] "CHAdeMO fast charging for EVs." [Online]. Available: http://www.chademo.com

[32] N. Haller and C. Metz and P. Nesser and M. Straw, "A One-Time Password System," 1998. [Online]. Available: https://tools.ietf.org/html/rfc2289