Secure Wireless Communication Platform for EV-to-Grid Research

Huaqun Guo
Institute for Infocomm Research,
A*STAR
1 Fusionopolis Way,
#21-01 Connexis (South Tower),
Singapore 138632
guohq@i2r.a-star.edu.sg

Fan Yu, W. C. Wong
Department of Electrical & Computer
Engineering,
National University of Singapore,
4 Engineering Drive 3,
Singapore 117576
{u0606010; elewwcl}@nus.edu.sg

Vivy Suhendra, Y. D. Wu
Institute for Infocomm Research,
A*STAR
1 Fusionopolis Way,
#21-01 Connexis (South Tower),
Singapore 138632
{vsuhendra; wydong}@i2r.a-star.edu.sg

ABSTRACT

"Vehicle to Grid" power or V2G will be a new green energy scheme that allows electricity to flow from Electric Vehicles (EVs) to power lines. The objective of this paper is to design and develop a secure wireless communication platform for V2G research, with the aim to develop a suitable wireless test bed for the V2G in Singapore. First, this paper presents our system block diagram and required methods design which include V2G architecture design, integrated OBU (on-board unit) design, base station (Aggregator), Telematics, V2G authentication protocol, and schedule optimization of EVs against Grid conditions. It then focuses on the authentication protocol for secure wireless communications between the Aggregators and EVs. It addresses the new and special challenges related to EVs, such as large overhead and latency, which are crucial for secure wireless communications with dynamic and fast moving EVs. Finally, the paper presents the initial test results and shows that our authentication protocol can securely protect the exchanged information with less overhead and less authentication latency.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General - *Data communications, Security and protection.*

General Terms

Algorithms, Performance, Design, Experimentation, Security, Verification.

Keywords

Secure wireless communication; electric vehicle; power grid; authentication protocol

1. INTRODUCTION

Vehicle-to-grid (V2G) describes a system in which electric or plug-in hybrid vehicles communicate with the power grid to sell demand response services by either delivering electricity into the grid or by throttling their charging rate [1, 2]. For example, Electric Vehicles (EVs) have the energy source within them and power electronics capable of producing the 50 Hz AC electricity that can be used to power offices and homes. V2G power will be a new scheme that adds the connections to allow this electricity to flow from cars to power lines. Cars pack a lot of power and one typical EV can put out over 10kW, the average draw of 10 houses [3].

The concept of V2G that allows the electricity to flow from EVs to power lines is very new. The project will be enable building the first nationwide test bed in the world for V2G, a new green energy scheme. It will address new and special issues and challenges related to EVs, such as latency and authentication, which are the crucial for secure wireless communications with dynamic and fast moving EVs. Thus, the main objective of this paper is to design and develop a secure wireless communication platform for EV-to-Grid research, with the aim to develop a suitable wireless test bed for the V2G in Singapore.

The system block diagram is shown in Fig. 1. The scenario of V2G is that the Power Aggregator, which obtains the electricity requirement instruction from the Control Center, will send out messages to call the EVs within a certain distance. The EVs will respond if EVs want to sell back the electricity to the Aggregator. As shown in Fig. 1, the wireless communications will involve the Aggregator, EVs, and the Control Center. Global Positioning System (GPS) signals from satellites are used to determine the location of EVs and guide the EVs to the Aggregator.

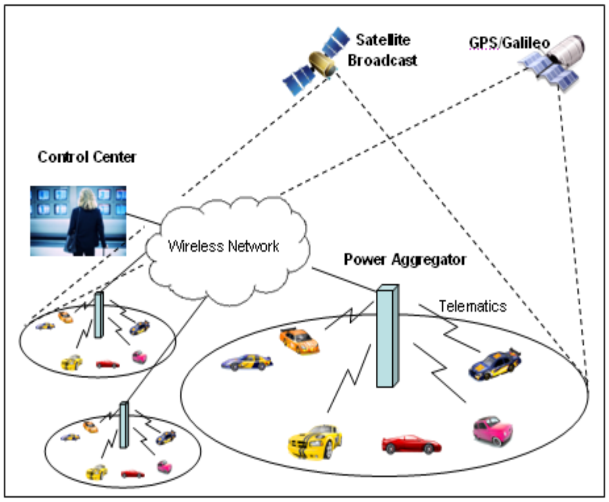

Figure 1. Ssytem block diagram for V2G

The remainder of this paper is organized as follows: The background is presented in the next section. We describe our methods design for EV-to-Grid research in Section 3. Section 4 presents the drawback of the traditional PKI-based authentication protocol and hence presents our Hybrid authentication protocol, while Section 5 presents the initial test of our algorithm. Finally, Section 6 outlines our conclusions and future works.

2. BACKGROUND

V2G will enable EVs or hybrid EVs with battery to plug into the power grid. Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the vehicles to the power lines and back. The ability of the V2G car's battery to act like a sponge provides a solution for utilities, which pay millions to generating stations that help balance the grid with a value to the utilities of up to $4,000 per year per car [4, 5].

There are currently a number of groups on V2G research. One notable V2G project in the United States is at the University of Delaware, where a V2G team has been conducting on-going research. Their goals are to educate about the environmental and economic benefits of V2G and enhance the product market [3, 5]. Other researchers and companies are the Pacific Gas & Electric Company, Google, Xcel Energy, the National Renewable Energy Laboratory, and, in the United Kingdom, the University of Warwick [5, 6].

3. METHODS DESIGN

In this section, we present the required methods design for EV-to-Grid research. The communications between the Aggregator and the EVs, and between the Aggregator and the Control Center will be realized through 3.5G mobile broadband communication. The security requirements include authentication of EVs, privacy protection of EVs and owners, and preventing fake messages, replaying message and eavesdropping. The information that the Power Aggregator needs from EVs includes ID of EVs, battery voltage, battery chemistry type, temperature, charging profile (how much available), driving habit, etc. Fig. 2 illustrates the methods which will be deployed in this project. The scope of this project includes the following six aspects.

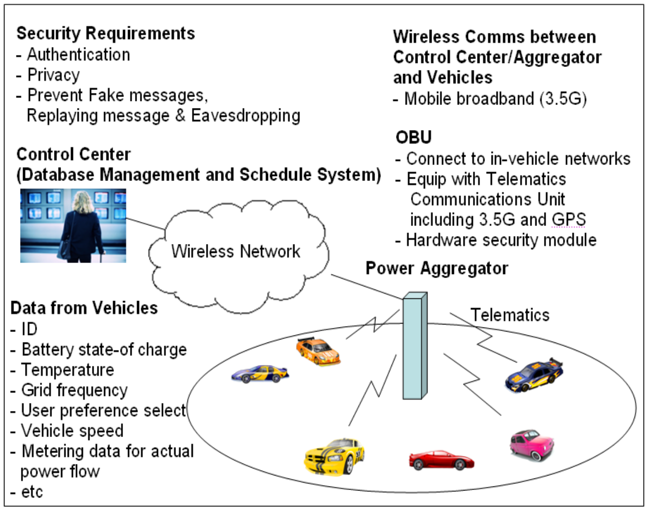
Security Requirements
- Authentication
- Privacy
- Prevent Fake messages, Replaying message & Eavesdropping
Wireless Comms between Control Center/Aggregator and Vehicles
- Mobile broadband (3.5G)
OBU
- Connect to in-vehicle networks
- Equip with Telematics Communications Unit including 3.5G and GPS
- Hardware security module
Control Center
(Database Management and Schedule System)
Wireless Network
Power Aggregator
Telematics
Data from Vehicles
- ID
- Battery state-of charge
- Temperature
- Grid frequency
- User preference select
- Vehicle speed
- Metering data for actual power flow
- etc

Figure 2. Methods of secure wireless communication for V2G

3.1 V2G Architecture Design

The R&D will investigate and design the V2G architecture which includes hardware requirements, communication system set up, and communication software design for the Aggregator, OBU and the Control Center.

In this stage, performance evaluations will be carried out in three aspects:

- Communications
  The project will evaluate whether there is difficulty in transmitting data between the Control Center, the Aggregator and vehicles; and whether information conveyed to vehicles by satellite is clear and precise.
- Delay
  The project will evaluate the latency to identify the location-based vehicles, and response time for vehicles' driving to the Aggregator.
- Accuracy
  The project will test and evaluate the accuracy of transmitting the information, determining the location-based vehicles, and guiding the vehicles to the Aggregator.

3.2 Integrated OBU Design

The R&D will investigate and integrate the OBU which will be purchased commercially and modified and will be embed in an EV. The OBU will connect to the in-vehicle networks to obtain real-time information about the status of the EV. The OBU will be equipped with Telematics Communications Unit including 3.5G mobile broadband communication and GPS antenna, receiver & transmitter. The OBU will have a tamper-resistant Hardware Security Module to store the private cryptographic key material, provide cryptographic functions (digital signature generation & decryption of encrypted messages), and provide key and device management functions.

Through the hardware and software design, the project will enable the OBU to obtain the following information:

- User secure identification
- Enable response signal
- Battery state-of charge,
- Temperature — too hot is not wanted
- Grid frequency — 50 HZ (< 48 HZ is not wanted)
- User preference select (discharge time, charged time, power discharged/ charged by 10 %, 20 % or 50%)
- Vehicle location e.g. zone, control area (using GPS)
- Charging station(s) location (GPS)
- Vehicle speed — how fast to plug in
- Driving pattern / history — very sensitive information (need to protect)
- Metering data for actual power flow (demand/supply), e.g. charging/discharging time, current, utility power rates.

3.3 Base Station (Aggregator)

The project will involve the software design for the Aggregator to communicate with OBUs in EVs and the Control Center together with the authentication protocol. The software will receive the power requirement from the Control Center and then call for EVs to buy back the power. It will also capture the number of EVs and measure the power using bi-directional power meters.

3.4 Telematics

Telematics is the integrated use of telecommunications and informatics, which is the specifically integrated use of GPS technology, computers and mobile communications technology in EVs. The project will design the telematics system which includes software development for Data Modules and data mining to process the data that the OBU obtains from various sensors and from ECUs (Electronic Control Units) inside an EV, Telematics software will be used for the transmission of data, voice and GPS geographic location information, and receiving information from the Aggregator and the Control Center.

3.5 V2G Authentication Protocol

The project will design authentication protocols with symmetric key cryptography and/or asymmetric key cryptography for the authentication between EVs and the Aggregator/Control Center, develop the software on both EV and the Aggregator, and evaluate the performance. It will propose a new authentication scheme and key exchange protocol that takes into account the limitations and capabilities of the OBU/Aggregator. It will investigate the performance of open-source authentication protocols vs. our proposed authentication protocols, and study and evaluate storage requirement and usage of secure key.

3.6 Schedule Optimization of EVs against Grid Conditions

In this area, the project will monitor the Grid frequency, monitor the charging point operation on the number of EVs which are plugged into the charging points, and collect the position data on the location of charging points and EVs. The authentication protocol and security protection will be developed for the information exchanged between the charging points/EVs and Grid. Based on all the dynamic data collected from the EV parameters, traffic condition, Grid status, the key function of this task is to develop a database software management system to schedule and optimize V2G operation according to multi-functional criteria, i.e., cost, emission, time, efficiency, and reliability.

4. AUTHENTICATION PROTOCOL

4.1 Related Works

Currently there is the IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE). The WAVE standards define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. The IEEE 1609 Family of WAVE Standards consists of IEEE P1609.1 - Standard for WAVE - Resource Manager, IEEE P1609.2 - Standard for WAVE - Security Services for Applications and Management Messages, IEEE P1609.3 - Standard for WAVE - Networking Services, and IEEE P1609.4 - Standard for WAVE - Multi-Channel Operations [7].

In IEEE 1609.2, to authenticate a message's sender and achieve the message's integrity, OBUs and RSUs should sign the messages with their private keys before sending the messages. The format of a signed message is shown in Fig. 3, where a 125-Byte certificate and a 56-Byte Elliptic Curve Digital Signature Algorithm (ECDSA) signature have to be attached for each 69-Byte message [8]. Thus, the cryptographic overhead (the certificate and the signature) takes up a significant portion of the total packet size [9].

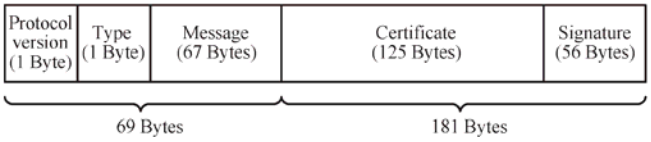

Figure 3. Format of a signed message

In [10], vehicular communication systems adopt the traditional public key infrastructure (PKI)-based security scheme. The sender calculates a signature using its private key and also attaches its certificate. The receiver can verify the message signature using the sender's public key in the attached certificate, which can be verified using the pre-installed public key of Certification Authority (CA). Again, the cryptographic overhead is big too.

In addition, the cryptographic algorithms with public key cryptography perform at relatively slow speeds [11].

4.2 A Hybrid Authentication Protocol

In this protocol, we use a hybrid authentication scheme. The main idea is that first we use a PKI for the communication between the Aggregator and EVs to establish shared secret keys; next, the subsequent communications use the shared secret keys for the encryption and decryption of data so as to reduce the cryptographic overhead since the public keys and public keys certificates are significantly larger than the shared secret keys.

In our scheme, both Aggregators and EVs share a common trust point that they both use the same CA such as Land Transportation Authority to have their certificates signed. The steps for the secure communication between an Aggregator and an EV are listed below. In those steps, $\|$ is the message concatenation operation, which appends in a special format; $\{M\}_{key}$ is to encrypt or decrypt the message M using the corresponding *key*, S is a signature using the corresponding secret key, and H(.) is a one way hash function, like SHA-1.

(1) An Aggregator signs a message (M_A) using its private key *SKA* and attaches its certificate C_A to call the EVs for electricity: $M_A \| C_A \| S_{SKA.}$

(2) An EV in a nearby location receives the message and uses the Aggregator's public key *PKA* which is in the attached certificate to verify that the message is from the Aggregator: $\{ S_{SKA}\}_{\mathrm{PKA}} = \mathrm{M_A}$

(3) The EV decides to provide its electricity and thus it establishes a shared secret key *SSK* with the Aggregator using the Diffie-Hellman key exchange algorithm [12].

(4) Now the shared secret key *SSK* is established between the Aggregator and the EV. The following communication between these two parties will use the shared secret key.

(5) The EV sends the information (M_I) that the Power Aggregator needs, which is shown Fig. 2, together with the ID of EV, *IDE*, and timestamp, *TS*: $H(IDE, \{TS \| M_I\}_{SSK}) \| \{TS \| M_I\}_{SSK}$. The hash function H is used to protect the privacy of the EV and the timestamp *TS* is used to prevent replay attack and the *IDE* is used by the Aggregator to look for the right shared secret key to decrypt the message.

(6) When the Aggregator receives the message from the EV, it uses the IDs of EVs to hash the received encrypted message to find out the right vehicle *IDi*: $H(IDi, \{TS \| M_I\}_{SSK}) = H(IDE, \{TS \| M_I\}_{SSK})$. Hence, after getting the vehicle *IDi*, the Aggregator obtains the corresponding right shared secret key *SSK* to decrypt the

message: $\{\{TS\|M_I\}_{SSK}\}_{SSK}= TS\|M_I$. Finally, the Aggregator obtains the required information M_I from the EV.

(7) The Aggregator then sends an acknowledgement message to the EV.

(8) Steps 5 to 7 are repeated until all information from the EV are securely received and authenticated by the Aggregator.

(9) After the Aggregator receives all information from the EV and finds that the EV is eligible to supply the electricity, the Aggregator encrypts a confirmed message (M_c) together with the timestamp TS using the shared secret key SSK and sends it to the EV: $\{TS\|M_c\}_{\mathrm{SSK}}$.

(10) The EV decrypts the confirmed message using the same shared secret key: $\{\{TS\|M_c\}_{SSK}\}_{SSK}= TS\|M_{\mathrm{c}}$. Finally, the EV will be driven toward the Aggregator for the electricity supply.

5. EXPERIMENTAL RESULTS

The quickest and easiest way to secure a TCP-based network application is with SSL (Secure Sockets Layer) [13]. Thus, we adopt the OpenSSL Open Source toolkit [14] to implement the traditional PKI-based security scheme. We then implement our hybrid scheme and compare the performances in terms of overhead and message authentication delay.

5.1 Communication Overhead

As shown in Fig. 3, the communication overhead in the traditional PKI-based security scheme includes the certificate and signature. For our hybrid scheme, Steps 1 and 2 are the same as the traditional PKI-based scheme. From Step 4, all the following communications use a shared secret key and no longer attach the certificate and signature. Thus, the overhead is greatly reduced.

5.2 Message Authentication Delay

Message authentication delay (completion time) is from the time of the Aggregator's call to the Aggregator receiving and decrypting all responding messages from the vehicles.

We carry out experiments using our proposed hybrid scheme, compared to the standard PKI-based ECDSA scheme in [8], and RSA scheme [15]. In our experiments, we adopt the OpenSSL Open Source toolkit and run the software for the traditional PKI-based security scheme using the RSA algorithm and the ECDSA scheme. In our hybrid security scheme, we use Diffie-Hellman algorithm to establish the shared secret key and then use Blowfish [16], which is a keyed, symmetric block cipher for data encryption and decryption. We made a *for* loop in each system so that vehicles will send messages multiple times, respectively.

In the first experiment, we use the message size of 69 bytes to test with three schemes respectively. The number of messages is varied from 1000 to 5000. The results are shown in Fig. 4. From Fig. 4, it is clear to show that the authentication delay in the hybrid scheme is the smallest; the authentication delay in ECDSA is medium, while the delay in the RSA scheme is the largest. There are some reasons for those results. (1) Key size: NIST (National Institute of Standards and Technology) guidelines state that ECC keys should be twice the length of equivalent strength symmetric key algorithms [17]. So we use 192 bits shared key size for the hybrid scheme, use 384 bits ECC key size for the ECDSA scheme, and 2048 bits key size for the RSA scheme. (2) Overhead: The hybrid scheme uses a shared secret key instead of attaching the certificate and signature, while the PKI-based ECDSA scheme and RSA scheme need to attach the certificate and signature. (3) Computational time and transmission time: Because of the smallest key size and overhead, the computational time and transmission time in hybrid scheme are reduced greatly. Therefore, the total completion time in the hybrid scheme is the smallest.

Next, we carry out more intensive tests for various message sizes and message number for three schemes, respectively. The results are shown in Figures 5, 6, and 7 respectively. From three figures, it also clearly shows that the completion time in the hybrid scheme is the smallest and the completion time in the RSA scheme is the largest. Furthermore, these figures also indicate that the message sizes are not the dominant factors. The completion time is more affected by the number of messages. The reason is that the more messages to be exchanged, the more time saved with the smallest key and overhead are achieved.

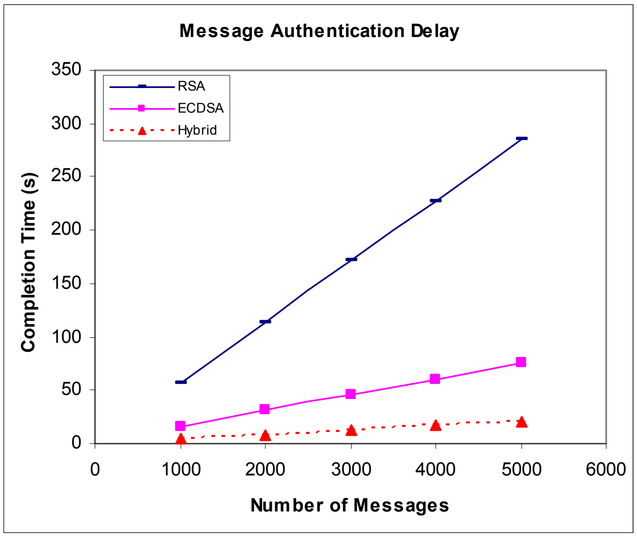

Figure 4. Message authentication delay for three schemes

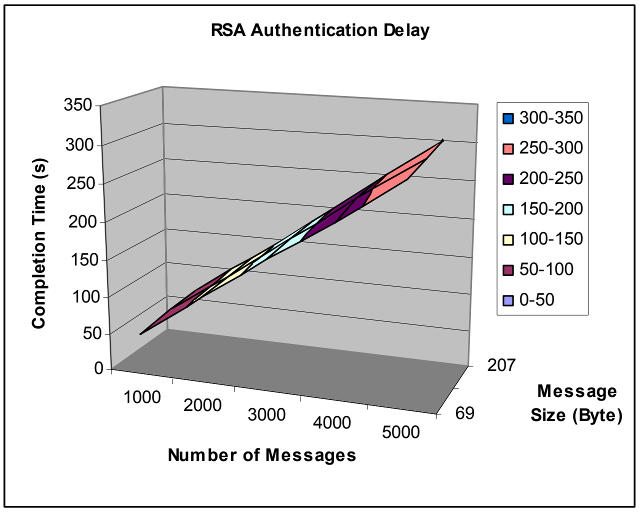

Figure 5. Effect of message size and number of messages on RSA authentication delaty

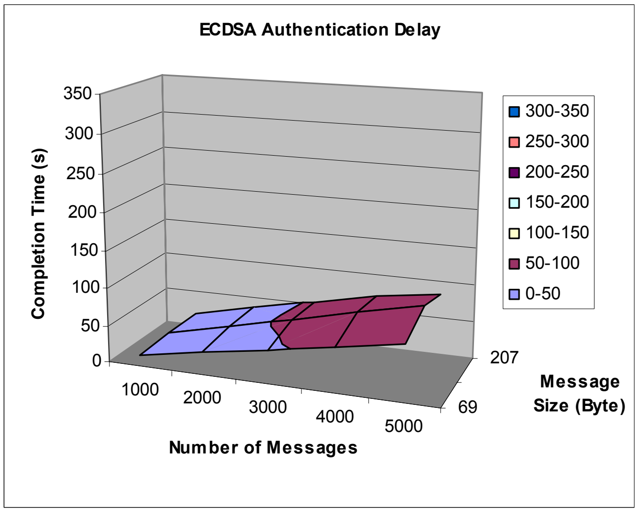

Figure 6. Effect of message size and number of messages on ECDSA authentication delaty

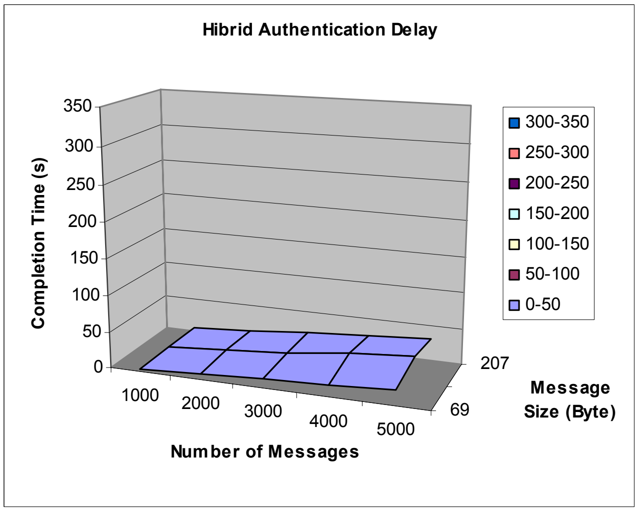

Figure 7. Effect of message size and number of messages on Hybrid authentication delaty

In summary, the experimental results prove that our hybrid scheme can reduce the authentication delay.

6. CONCLUSIONS

In this paper, we propose a secure wireless communication platform for V2G research, with the aim to develop a suitable wireless test bed in Singapore. We describe the methods design for EV-to-Grid research which includes the V2G architecture design, integrated OBU design, Aggregator software design, Telematics design, V2G authentication protocol, and schedule optimization of EVs. We then focus on the design and development of a hybrid authentication protocol which uses the PKI-based scheme to establish a shared secret key and then uses the shared secret key to fast encrypt and decrypt the messages so as to meet the challenges of the highly dynamic vehicular communication. The experimental results show that our hybrid scheme can reduce overhead and message authentication delay.

In the future, we will continue the R&D of the whole system, including the hardware and software design and implementation, and evaluate the various performances.

7. REFERENCES

[1] Cleveland, C. J. and Morris, C. 2006. Dictionary of Energy. Amsterdam: Elsevier. , pp. 473, 2006.

[2] Pacific Gas & Electric. 2007. Pacific Gas and Electric Company Energizes Silicon Valley With Vehicle-to-Grid Technology. April 2007. Retrieved 16 December 2009 from http://www.pge.com/about/news/mediarelations/newsreleases/q2_2007/070409.shtml.

[3] V2G Home. 2009. What is V2G?. Retrieved 14 December 2009 from http://www.udel.edu/V2G/.

[4] Science Daily. 2007. Car Prototype Generates Electricity, And Cash. December 9 2007. Retrieved 16 December 2009 from http://www.sciencedaily.com/releases/2007/12/071203133532.htm.

[5] Vehicle-to-grid. 2009. Retrieved 16 December 2009 from http://en.wikipedia.org/wiki/Vehicle-to-grid.

[6] Motavalli, J. 2007. Power to the People: Run Your House on a Prius. New York Times, September 2 2007. Retrieved 16 December 2009 from http://www.nytimes.com/2007/09/02/automobiles/02POWER.html.

[7] U.S. Department of Transportation. 2009. IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE). ITS Standards Fact Sheets, September 25, 2009. Retrieved 2 September 2008, from http://www.standards.its.dot.gov/fact_sheet.asp?f=80.

[8] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages, IEEE Std. 1609.2-2006, July 2006.

[9] Zhang, C., Lin, X., Lu, R., Ho, P.H., and Shen X. 2008. An Efficient Message Authentication Scheme for Vehicular Communications. IEEE Trans. on Vehicular Technology, Vol. 57, No. 6, pp. 3357-3368, 2008.

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

[11] Weise, J. 2001. Public Key Infrastructure Overview. Sun BluePrints Online, August 2001. Retrieved 16 December 2009 from http://www.sun.com/blueprints/0801/publickey.pdf.

[12] Diffie-Hellman Key Exchange. Retrieved 16 December 2009 from http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange.

[13] Rescorla, E. 2001. An Introduction to OpenSSL Programming (Part1). LINUX Journal, October 2001. Retrieved 16 December 2009 from http://www.linuxjournal.com/article/4822.

[14] OpenSSL. Retrieved 16 December 2009 from http://www.openssl.org/.

[15] Mao, W. 2004. Modern Cryptography Theory & Pracrice. Prentice Hall Professional Technical Reference, New Jersey, USA, 2004.

[16] Blowfish. Retrieved 16 December 2009 from http://en.wikipedia.org/wiki/Blowfish_(cipher).

[17] Key size. Retrieved 16 December 2009 from http://en.wikipedia.org/wiki/Key_size.