DESIGN OF RFID MESH NETWORK FOR ELECTRIC VEHICLE SMART CHARGING INFRASTRUCTURE

Contributors:

Ching-Yen Chung, Aleksey Shepelev, Charlie Qiu, Chi-Cheng Chu, and Rajit Gadh
Smart Grid Energy Research Center
University of California, Los Angeles, USA

Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000192.

Disclaimer

Design of RFID Mesh Network for Electric Vehicle Smart Charging Infrastructure

Ching-Yen Chung, Aleksey Shepelev, Charlie Qiu, Chi-Cheng Chu, Rajit Gadh
Department of Mechanical and Aerospace Engineering
University of California, Los Angeles
Los Angeles, USA
chingyenchung@ucla.edu, ashepelev@ucla.edu, qiucharlie@gmail.com, peterchu@ucla.edu, gadh@ucla.edu

***Abstract*—With an increased number of Electric Vehicles (EVs) on the roads, charging infrastructure is gaining an ever-more important role in simultaneously meeting the needs of the local distribution grid and of EV users. This paper proposes a mesh network RFID system for user identification and charging authorization as part of a smart charging infrastructure providing charge monitoring and control. The Zigbee-based mesh network RFID provides a cost-efficient solution to identify and authorize vehicles for charging and would allow EV charging to be conducted effectively while observing grid constraints and meeting the needs of EV drivers.**

Keywords—Electrical vehicle charging, power distribution control, smart grids, RFID, Wireless LAN, wireless mesh network, Zigbee

I. INTRODUCTION

As the number of EVs on the roads increases, charging stations in both parking structures and private garages will become more prevalent. These stations will be responsible for meeting the requirements of the distribution grid, EV owners, and parking structure operators. For security and financial reasons, among the many functions these charging stations will perform are user authorization, authentication, and billing.

Basic, unnetworked, charging stations such as Leviton[1] and ClipperCreek[2] require a point of sale (POS) device to authorize and enable charging. Other commercial charging stations, such as Coulomb[3] and Blink[4] require a short range RFID card for the same purpose. In both cases, extra steps on the part of the user must be taken to authorize charging. The authors in [5] propose using conventional RFID tags inside EVs and RFID readers on parking garage access gates together with middleware and an aggregate charging controller to authorize, assign, and enable charging. However, this system still requires action from the user and is not as flexible as may be desired.

The UCLA Smart-Grid Energy Research Center (SMERC) has developed a software-based EV monitoring, control, and management system that employs multiplexed charging stations capable of providing varying power to several EVs from one circuit, called WINSmartEV^{TM}[6][7][8]. This system centers around a server-based aggregated charging controller and utilizes a user database together with a smart-phone interface for charging authorization.

In order to simplify the charging authorization process and make it more convenient for users, an authentication system based on an RFID mesh network is proposed as an additional capability for the existing WINSmartEV^{TM} framework. The proposed improvements allow charging authorization to take place seamlessly at multiple charging stations in a single geographic location without any action on the part of the user. Vehicle Monitoring/Identification Modules (VMMs), located in EVs, act as RFID tags for vehicle identification and charging authorization. Unlike the layered architecture for managing a variety of automatic identification hardware proposed in [9], the VMMs communicate directly with a network coordinator and charging control server through a ZigBee mesh network, thus simplifying the architecture.

The paper is structured in the following way: first, the existing WINSmartEV^{TM} architecture is outlined. Then the architecture of new Zigbee-based RFID charging authentication system is presented and each component of the system is described in detail. Last, the results of the implementation are presented and discussed.

II. EXISTING WINSMARTEV^{TM} SYSTEM

This section introduces the WINSmartEV^{TM} smart-charging infrastructure, the existing network architecture as well as the design of the WINSmartEV^{TM} smart-charging station. Fig. 1 shows a WINSmartEV^{TM} four-channel smart charging station in a UCLA parking garage.

Figure 1. Installation of 4-channel smart charging station

The charging station supports variable-current charging of multiple EVs at one time. Currently, an authorized user is able to check available charging stations, start or stop EV charging, check the charging status, view monthly charging records, and manage user account via a mobile device. A screen shot of the mobile app used is shown in Fig. 2.

Figure 2. Screen shots of User Control Center

The network architecture of the WINSmartEV^{TM} smart-charging infrastructure is illustrated in Fig. 3.

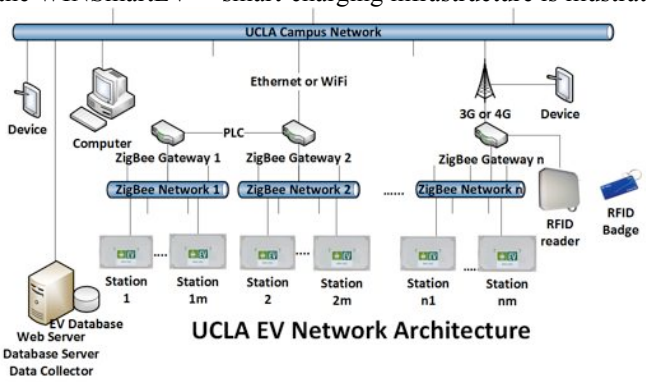

Figure 3. WINSmartEV^{TM} Infrastructure

A server-based aggregate charging control system controls all charging stations through multiple protocol gateways with 3G connection. 3G communication is necessary due to its applicability anywhere a cellular signal exists, especially where wired or WiFi communication is unavailable. The communication methods used within a single charging station are detailed in Fig. 4

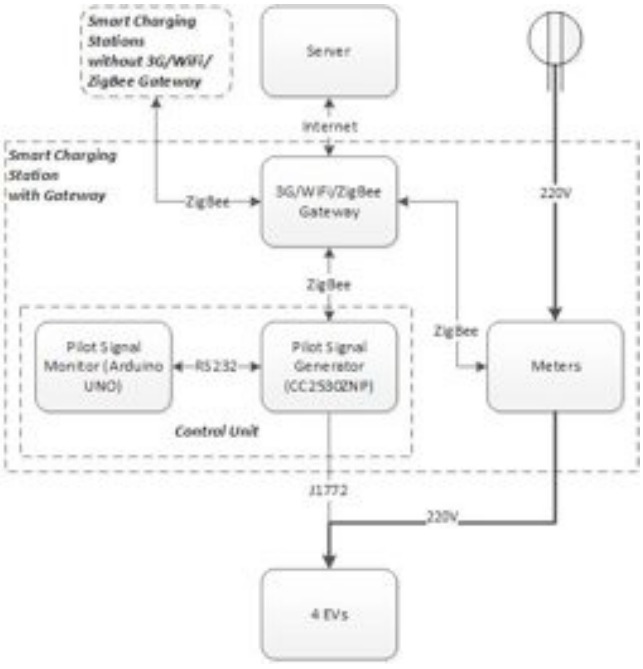

Figure 4. Details of smart charging station

ZigBee is used for communication between the gateway, meters, and the control unit in a single station as well as between a gateway-equipped master station and all other non-gateway-equipped stations in a geographic locale.

The aggregate charging control system is employed to monitor and control charging activities. There are four major software components in the system including: Database, Station Controller and Data Collector, System Monitoring and Control Center, and User Control Center. The Station Controller and Data Collector sends commands to the charging station to control charging while gathering and accumulating power information. A system administrator can manually control the charging stations through the Monitoring and Control Center shown in Fig. 5.

Figure 5. Screenshot of Monitoring and Control Center

III. Proposed Authorization System

The existing system requires the user to authenticate themselves through a mobile app. The new mesh network RFID charging authorization system proposed in this section, which requires no actions from the user, would add a new level of capability to the WINSmartEV^{TM} EV smart-charging infrastructure.

A. Zigbee-based RFID Mesh Network Architecture

The concept of Mesh Network RFID for charge authorization is shown in Fig. 6.

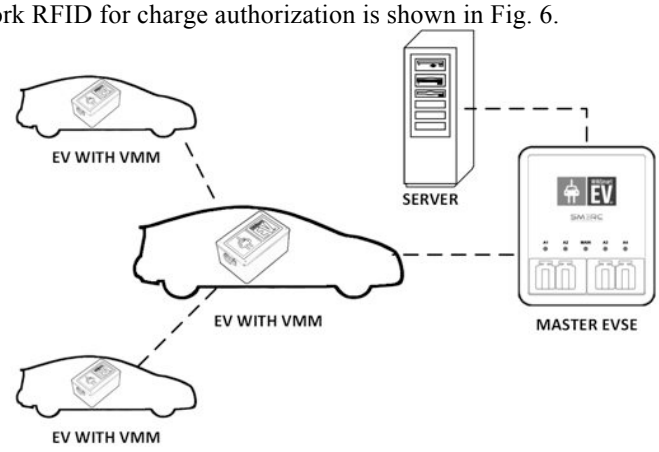

Figure 6. Mesh Network RFID with EV Smart-Charging Infrastructure.

The wireless mesh network consists of a Zigbee coordinator located in a central charging station and Zigbee routers located in each of the custom-made EV-mounted VMMs. The ZigBee coordinator, attached to the Gateway in the charging station, serves as the RFID reader while the ZigBee routers in the VMMs serve as RFID badges. The unique 64-bit MAC address of each ZigBee device allows it to be utilized as an RFID tag.

Data from the EVs may take any available path to the coordinator so that the condition of RF signal blocking by cars may be improved. This architecture allows only one Zigbee coordinator to be used for multiple charging stations in a parking garage. Despite the fact that each EV in the network draws power from its respective charging station, each EV transmits its data to a single master station, allowing all others to be simplified, thus reducing their cost.

In addition, because a number of control devices in each charging station can also communicate on the ZigBee mesh network, the charging stations can communicate with each other as well. Therefore, only one gateway is required in each localized area to service multiple charging stations and their respective EVs.

The Mesh Network RFID for the WINSmartEV^{TM} EV smart-charging infrastructure is developed based on existing hardware without additional cost and provides traditional RFID benefits of unique ID and wireless communication while adding mesh networking capability.

B. Charging Authentication with RFID

Charging authentication with the ZigBee RFID mesh network involves several processes including ZigBee MAC address retrieval, user authorization, and EV plug-in status detection, as shown in Fig. 7.

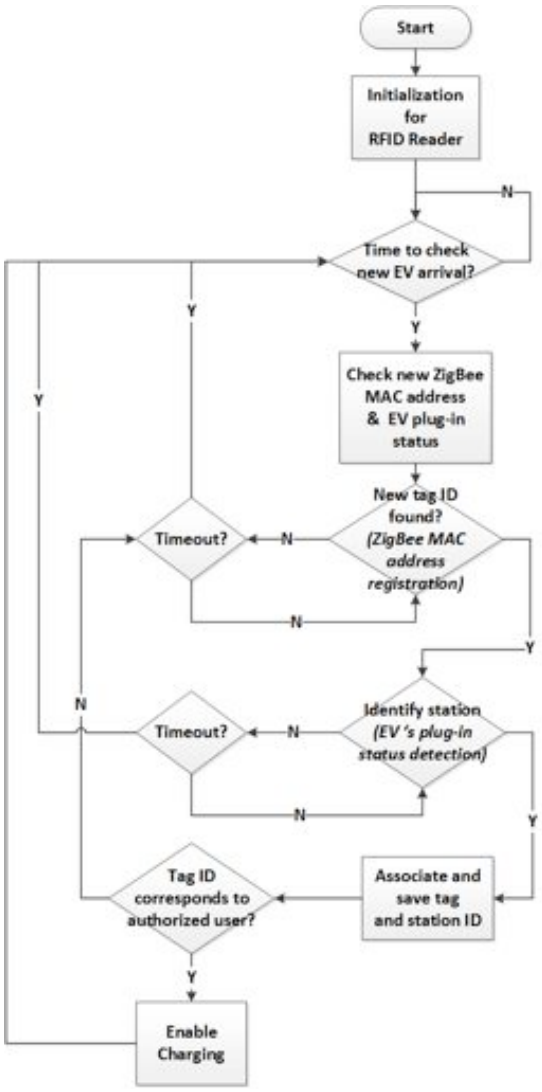

Figure 7. Charging authentication process using RFID

The charging authentication process checks new EV arrivals on a specific interval. After RFID reader initialization, the server sends out the "rgst" command to check if new ZigBee MAC addresses (tag IDs) have been registerred. The "stat" command is also sent out to identify which charging station a newly arrived EV is plugged into. If the tag ID corresponds to an authorized user account stored in the database, the server sends out the enable charging command to start EV charging. The commands from the server to the charging stations are in the format: ***comd[command] [channel] [parameter]***. The description of the commands and return values are summarized in Table I.

TABLE I. COMMANDS OF THE CHARGING STATION

Command	Description and Example
rgst	Return all registered ZigBee MAC address
	comdrgst0000 [return]: rgst01[MAC address][approach/leave/stay] rgst02[MAC address][approach/leave/stay]
stat	Charging station status request
	comdstat0100 request channel 1 status [return]: duty0150rely0101plug0101stat0100

C. RFID Reader: ZigBee Coordinator

The ZigBee coordinator serves as the RFID reader and handles messages between the gateway and the end devices/routers. When a ZigBee router joins the mesh network, the coordinator assigns it a 16 bits dynamic address and

associates the dynamic address with the unique MAC address of the ZigBee device. The coordinator unit is implemented using a CC2530ZNP with Max3232 as shown in Fig. 8.

Figure 8. ZigBee coordinator implementation

The ZigBee coordinator recognizes an approaching or departing EV by the Received Signal Strength Indication (RSSI) from the ZigBee router or ZigBee End Device.

In order to ensure a stable connection with each Zigbee device in the network, a handshake protocol has been implemented. The handshake between the RFID reader (ZigBee Coordinator) and an RFID tag (ZigBee router) is summarized in Table II.

TABLE II. ZIGBEE HANDSHAKE COMMANDS

Command	**Initiating Device**	**Format**
Request	ZigBee router	“comdtest[MAC address]”
Response	ZigBee coordinator	“comdresp[MAC address]”

The ZigBee coordinator firmware flow is shown in Fig. 9.

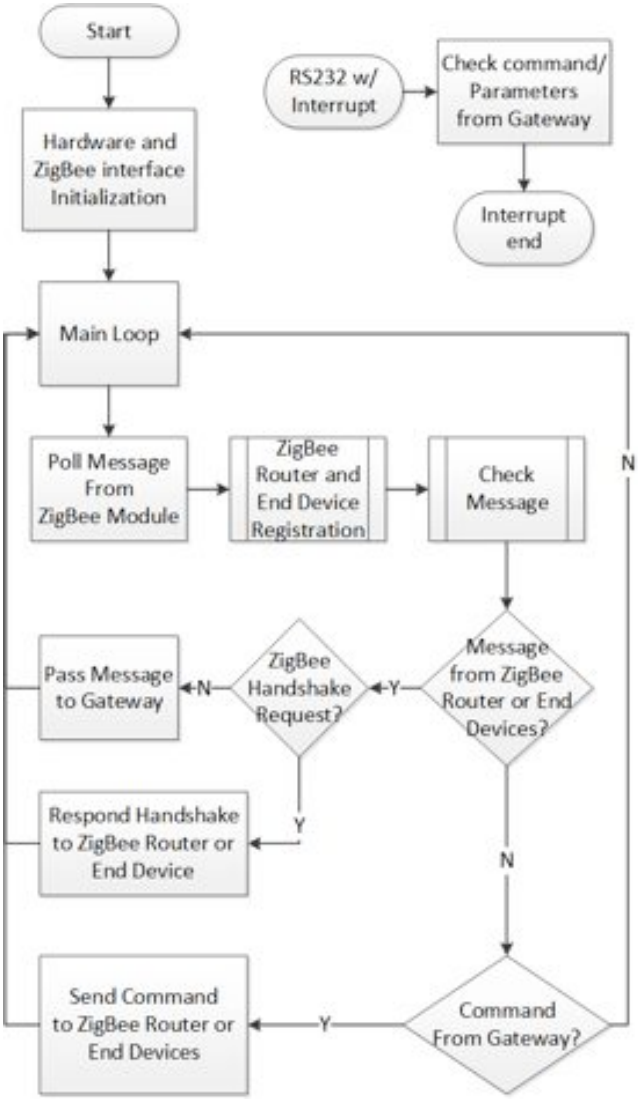

Figure 9. ZigBee coordinator firmware flow

D. RFID Tag: Vehicle Monitoring/Identification Module(VMM)

The role of the RFID tag is performed by a Zigbee-enabled remote monitoring module, known as the VMM, which is located in the EV. Just like a conventional RFID chip, the module has the capability of uniquely identifying each EV, with the ZigBee MAC address serving as the unique identifier. In addition, the module adds the ability to monitor EV states through the vehicle's CAN bus. This capability turns the VMM into a remote sensor in addition to being an RFID tag. Fig. 10 shows a schematic and a cutaway view of the VMM.

Figure 10. Schematic and cutaway view of VMM

The device employs a Texas Instruments ZigBee board equipped with an MSP430 microcontroller and a CC2530 RF transceiver for communication with the network coordinator node. To monitor the EV's CAN bus, the device uses an MCP2551 CAN transceiver chip and an Atmega328 microprocessor. Fig. 11 shows the firmware flow on the MSP430 microprocessor of the VMM.

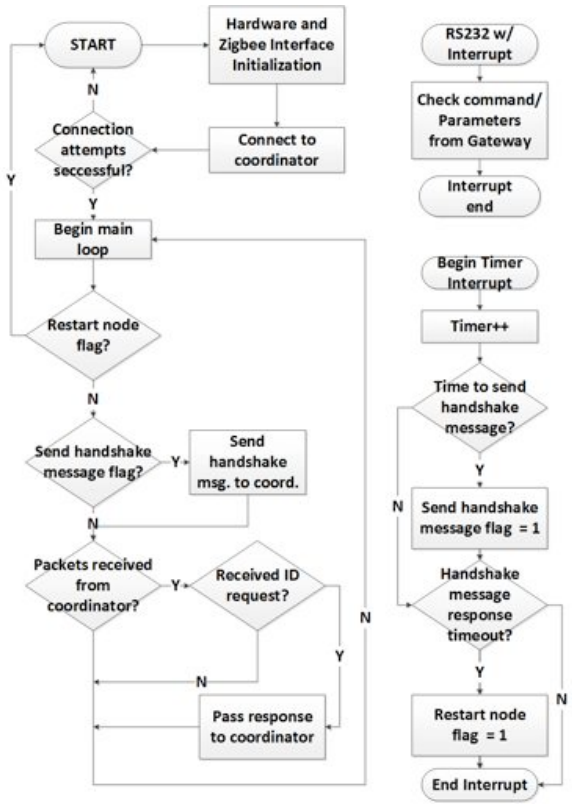

Figure 11. ZigBee node firmware flow in the VMM

The firmware is responsible for establishing a connection with the Zigbee coordinator, responding to ID requests, and maintaining the wireless connection by transmitting periodic handshake messages and restarting the node if no response is received to the handshake. The flowchart in the top right corner of Fig. 11 shows the logic of the timer interrupt located on the MSP430 processor. The timer interrupt is used primarily as a helper method for ensuring connectivity with the coordinator node. To this end, the interrupt keeps a running time count and uses it to sets flags that are later used in the main loop to transmit handshake messages or restart the node.

E. EV Plug-in Status Detection

EV plug-in status detection is used by the aggregate charging server to identify the presence of an EV at a charging station and to associate the vehicle's ID with a particular charge point. The hardware implementation of the smart charging station control unit with pilot signal generator/monitor is shown in Fig. 12.

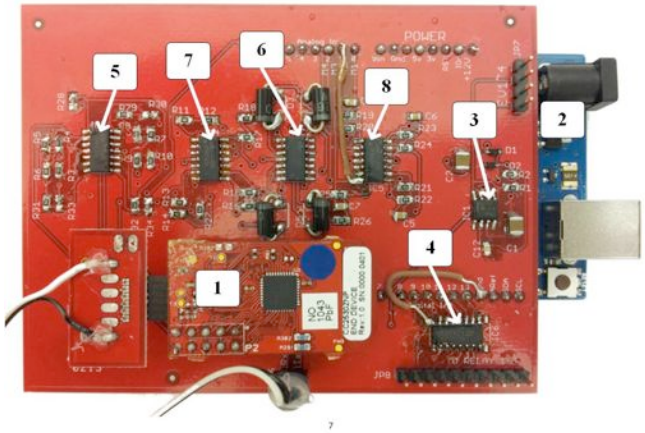

Figure 12. Implementation of the control unit: (1) Pilot Signal Generator (2) Pilot Signal Monitor (3) 555 counter. (4) Relay Driver. (5) Schmitt Trigger. (6) Unit Gain Buffer. (7) Inverting Amplifier. (8)Inverting LPF

A pilot signal generator/monitor circuit monitors plug-in status by detecting pilot signal voltage levels set by the EV. For monitoring purposes, the pilot signal is de-amplified to within the A/D converter's range and fed through a low-pass filter (LPF) to produce a DC voltage.

In addition to its monitoring capability, the circuit shown generates a variable duty cycle pilot signal that indicates available current to the EV as per J1772 specification.

The Pulse Width Modulation (PWM) pilot signal is produced by the pilot signal generator and amplified from 3.3V/GND to +/-12V by a Schmitt trigger when fed to the EV.

Before the aggregate server is notified of a status change, EV plug-in status detection is executed in the firmware-based state machine on the pilot signal monitor. Fig. 13 shows the state machine firmware flow.

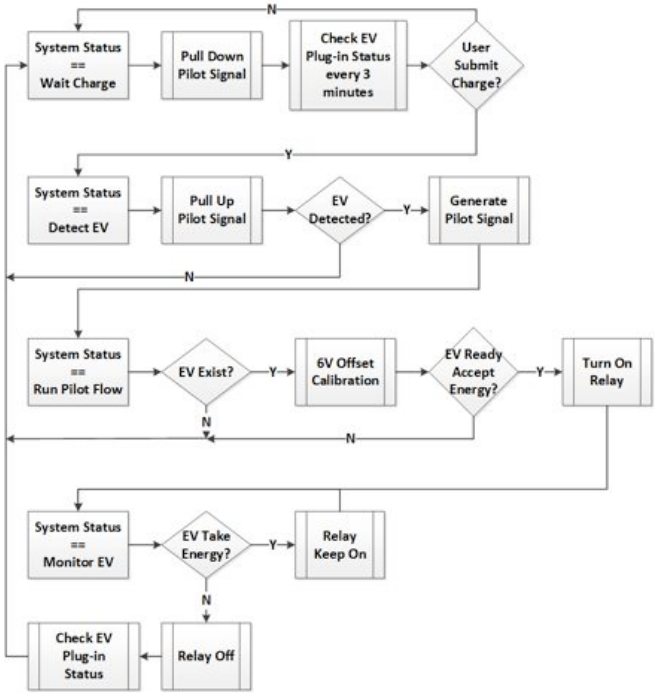

Figure 13. State Machine Flow of the Firmware

IV. Experiments and Results

Experimental results of EV plug-in status detection, RFID response time, and an RSSI tests are presented in the following sections.

1) EV plug-in status detection

In this experiment, the DC-converted pilot signal was measured at varying duty cycles for two distinct EV states: EV disconnected and EV charging. The experiment was performed with a Nissan Leaf charging at a 4-channel smart charging station shown in Fig. 1. The experimental results are shown in Fig. 14.

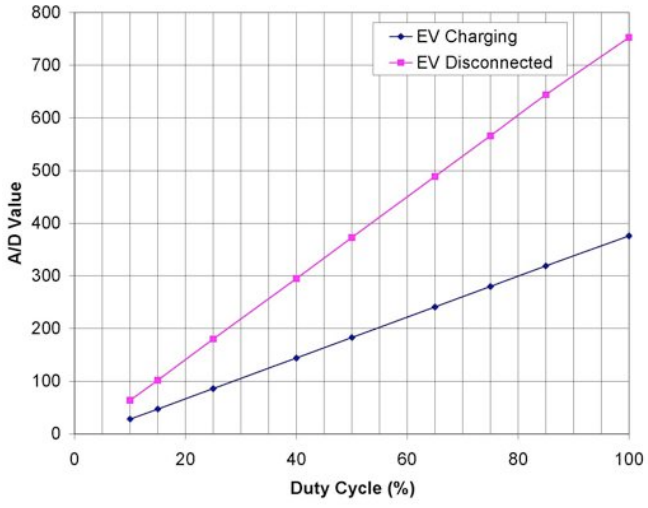

Figure 14. A/D Value v.s. Duty Cycle of Pilot Signal

The results show that the DC values seen at the A/D converter are clearly distinguishable in these two cases and have good linearity. Even when the duty cycle is around 10%, (or 6A-the minimum charging current set by the J1772 specification), the pilot signal monitor's resolution is still more than sufficient to detect the EV's plug-in status. The threshold value for EV plug-in status detection is set to be the average of these two cases.

2) RFID Response Time

The experimental setup of the RFID response time test is shown in Fig. 15.

Figure 15. Setup of RFID response time test

The response times for one-hop communicaton between a ZigBee coordinator and a ZigBee router are presented in Fig. 16.

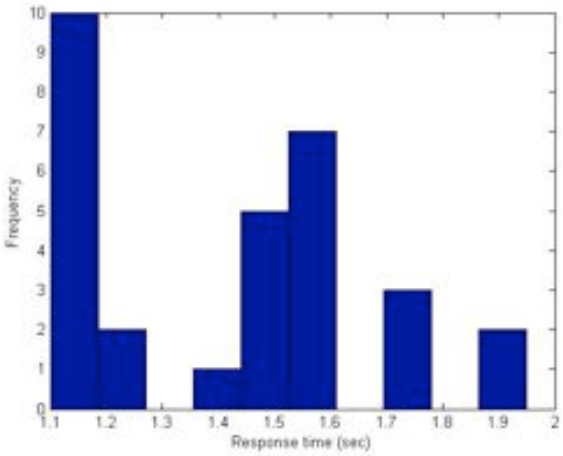

Figure 16. ZigBee router response times in 30 trial runs

The results show considerable variation in router response times, with an average delay being around 1.4 seconds. A two second minimum interval must be incorporated on the server to allow for message responses. An interval much larger than two seconds needs to be allowed for detecting an approaching EV.

3) RSSI Test

Fig. 17 shows the results of RSSI vs. distance between charging station and EV.

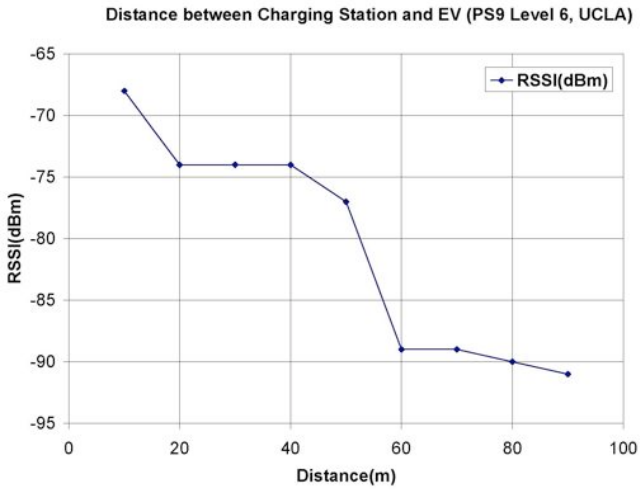

Figure 17. RSSI v.s. Distance between charging station and EV

The experiment shows that when the EV is within 50 meters of the charging station, the RSSI has a sudden jump -89 dBm to -77 dBm. Although the theoretical range for ZigBee communication is 75 meters, the charging station would detect the EV at 50 meters in the real world. Notice that the RSSI has another jump when the EV approaches within 20 meters, which implies that RSSI would be an appropriate metric for identifying an EV approaching a charging station.

The accepted speed limit in parking garage is 5 mph, which means an EV approaches a charging station by 4.5 meters every 2 seconds. After an EV is detected at a distance of 50 meters and assuming that the EV parks 5 meters away from the charging station, the station will have a maximum of 10 handshakes to determine whether the EV is approaching or leaving.

V. CONCLUSION

The ZigBee-based RFID charging authorization system presented in this paper provides a convenient method for a user to enable charging at a smart-charging station. The proposed system represents an improvement over the existing WINSmartEV^{TM} system as it allows charging authorization to take place seamlessly at the moment of EV arrival and does not require user involvement. An approach that utilizes a remote identification tag and charging station-based reader allows authorization/identification capability to be added to the existing WINSmartEV^{TM} charging infrastructure without excessive modifications in the underlying structure. Because EVs on the WINSmartEV^{TM} network are already equipped with remote tags for charge-state monitoring, adding authorization/identification capability is a matter of writing new firmware and software for existing hardware. The use of a mesh network allows a robust connection to be maintained between EVs and charging stations in a real world environment subject to signal blocking conditions. As a result of the aforementioned improvements, the new system brings SMERC research one step closer to an economical, and user friendly smart charging technology that enhances the stability and reliability of the local grid while meeting the convenience needs of EV drivers.

VI. ACKNOWLEDGEMENT

This work has been sponsored in part by a grant from the LADWP/DOE fund 20699 & 20686, (Smart Grid Regional Demonstration Project).

REFERENCES

[1] http://www.leviton.com/OA_HTML/SectionDisplay.jsp?section=37668&minisite=10251[03/20/2013]

[2] http://www.clippercreek.com/[03/20/2013]

[3] http://www.coulombtech.com/chargepoint-network.php[03/20/2013]

[4] http://www.blinknetwork.com/network.html [03/20/2013]

[5] S. Mal, A. Chattopadhyay, A. Yang, R. Gadh, "Electric vehicle smart charging and vehicle-to-grid operation", International Journal of Parallel, Emergent and Distributed Systems, vol. 27, no. 3. March 2012.

[6] Rajit Gadh et al., "Smart Electric Vehicle (EV) Charging and Grid Integration Apparatus and Methods," PCT International Patent, Ser. No. PCT/US11/40077, June 10, 2011

[7] Rajit Gadh et al., "Intelligent Electric Vehicle Charging System", PCT International Patent, Ser. No. PCT/US12/49393, August 2, 2012.

[8] C. Chung, P. Chu, R. Gadh, "Design of Smart Charging Infrastructure Hardware And Firmware Design of The Various Current Multiplexing Charging System," Seventh Global Conference on Power Control and Optimization PCO2013, Prague, 25-27 August, 2013

[9] X. Su, C. Chu, B.S. Prabhu, and R. Gadh "On the Identification Device Management and Data Capture via WinRFID Edge-Server", IEEE Systems Journal, 1(2), Dec 2007, 95-104.