# Electric Vehicle and Charging Station Technology as Vulnerabilities Threaten and Hackers Crash the Smart Grid

S.Ahmed, F. M. Dow

***Abstract*—**In recent years, an executive number of attacks is to be advanced the power system knowledge that may be able to create an integrity over the world. Wisely The security development of charging stations becomes urgent matters. The attention of smart grid and integrate different technology such as The quality of electric vehicles on the road increases more and more interesting. For example, Charging point is as part of smart grid. Greatly increases the massive risk to other functioning of the internal charge point that must be protected from external connections, it has an impact negatively on the smart grid and cyber-attacks are increasing quickly. The cyber terrorists are seeking to find new components in order to ensure protection its, it is necessary to detect vulnerabilities in critical systems before terrorists, or other adversaries are able to exploit them. To destroy an electric power infrastructure that is considered the backbone of each activity by attacking its wireless control system through cyber means has become an important way to weaken as platform cyber-attack in energy systems. In this paper we provide the charge station as platform to attack malicious programs and others attack the energy networks, a concept that explains How can I use the charge station technology equipped with all technical connections and software as the point exploits attack on sensitive areas with in management energy, The Attacks aim to exploit resources by sending unlimited fake requests to the smart grid. We further breakdown the charge station technology for communication and application infrastructure as the part of the research paper. On the other hand. We present the background and motivation of charge station infrastructures against vulnerabilities threaten and hackers crash in smart grid systems. Since a smart grid system might hold over millions of unsafe charge point and electric vehicle, We further had explored the charge station technology for wireless communication and application infrastructure as the part of a complex smart grid system.

***Index Terms*—**Charge point, vulnerability, smart grid, communication technology.

## I. Introduction

Smart grid technology is Machine-to-Machine (M2M) as a paradigm is defined as a new technology for the next generation of communication where a large number of intelligent machines share information and collaborate to make decisions without the human intervention. There is a greater need for electric vehicle infrastructure. As the number of electric vehicles(EVs) on the road increases more and more. One of the important manufactures is wireless technology. There are charging stations and his spot charger in the world. Public charging stations are vital, and such like are helping to extend the electric range of electric vehicles. Therefore, the number of electric vehicle operators will increase and make them more viable for long-range trips. , this smart grid will be necessary to build a sufficiently dense network of charging stations, These are required the deployment of charging stations that can be wherever located, in airports, shopping malls, as well as less controlled places such as curbs, roadside or on highways[2]. The smart communication of infrastructure links EVs with Electric Vehicle Supply Equipment (EVSEs). EVSE units are commonly referred to as “charging stations.” that provide a sensitive means to exchange such basic information, the combination in the future may be used for energy trading, bids and much more information that is useful for advanced smart grid applications [3]. Safety and IT are to prevent hazardous operation on the security measures, from discovering vulnerabilities, which are already being part of the Smart Grid machine, So that the mismatch between the connected physical device and the cyber authenticated on EV. This situation needs to be enhanced to cover also the Smart Grid access infrastructure as an electric vehicle charging station technology EV, EVSEs and Smartphone application are methods to the risks to the smart grid. Therefore Physical security the power grid may be the biggest risk if when the attackers launch attacks from EVs or EVSEs, Smartphone application where the driver uses some Features [4]. A Generally. Two-way of interactive technology between interested users, smart grid and wireless control applications, the neglects of security intention become complex tide to fail control technology of the electric vehicle charging station. In fig (1)electric vehicle charging station technology under the smart grid transmitted by communication technology. Physical tampering, malicious software uploads and load alteration are among the possible attacks on the EVs or EVSEs Smartphone [5]. While the most vulnerable part of the smart grid, Malware attackers loaded to an EVSE which can compromise an EV, easily from the worms can be carried from one to others around a city and its interconnections, as an EV travels and charges have its battery from several other EVSEs on the road.

The complex of this paper is organized as following: The electric vehicle is described In Section II. Components of charge station system . In Section III.smartgrid security. in section IV hackers crash concerns are viewed. In Section V. Charaing station vs vulnerabilites .In Section VI Threats and

S.AHMED, Higher Institute of Technology, Regdleen, Libya
F. M. Dow Libyan Authority for research, science and technology, Tripoli, Libya).

http://dx.doi.org/10.17758/EAP.EAP816010

vulnerabilities inside charging station meters.. In Section VII. Charger poles attack and types of attackes. Finally Conclusions in Section VIII.

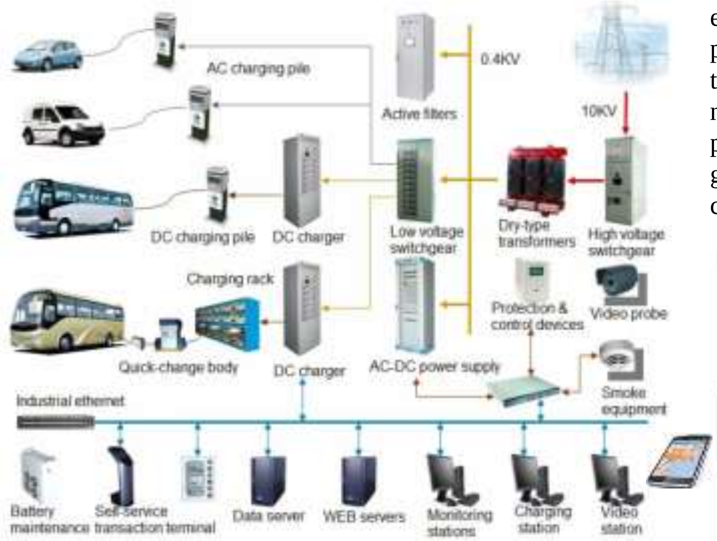

Fig.1 Technologies for electric vehicle charging station (10)

## II. Components of Charging Station System

The charging infrastructure of the electric vehicle generally consists a combination of wireless power services and security information . those components in charging station are LCD, electric circuit board, wireless networks communications (WIFI points, cellphone network, Bluetooth, smart grid, charging cord protocols). In point view charging stations are like electric poles in the street if there are no security technology, they are communicate to present safe information over the internet and using protocols to talk sensitively to charging station network, updating of data is transmitted on charging stations through various network protocols. However, The drivers can be needed incentive plan for utilising security of billing prices, control of the data charging is loaded to suffer various security threats. So that to reduce interrupted charging is based on smart grid components and state of EV's chargingnetwork access: physical access is to enter wireless devices that vulnerabilities as the attackers can look for unsafe communication. It is not possible of The carrying data and communication where identifiers of charging cards could easy to fake information identifications on charging components Configuration: it is not a perfect way of security. The connect to the components that are a laptop to Ethernet and setup web browser or denial of service. In addition. Insecurity piece of charging poles commonly is actual dangers on smart grid .

2- Application access to charging station such as EVSE is payment system may be utilised to collect data, it also is combined payment and data collection communications for instance Mobile Application, EVSE grow up invoice capacity( and many others) will need network communications, to be sure to confirm whether the EVSE requires Ethernet (Cat5 or Cat6) or cell grid access and schedules due to RS485 so that there is no insecurity of this channeled , that is commonly utilised between gizmos in the components .In reality, let's see if the station is ability or in engage to ensure you never navigated to busy station start .charging starts and charging stops with one tap notices, gaining real-time updates through your charging situation, to check miles of charging status must be based on Electric Vehicles Categories. The price of costing on your energy sessions depends since you have been plugged charge point, House schedule, EV's track usages.Map viewing and travel to thousands of charging positions from whole charging networks. Satellite can be displayer charging stations to the parking spot; Navigator will find your directions so you need to get information and details like real-time, pricing billing, the control output of charging locations.

.

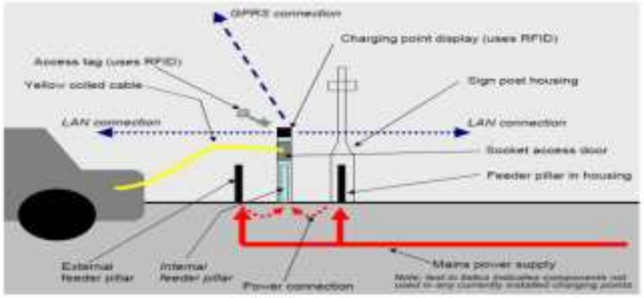

Fig 2. Components of charging point (12)

## III. Smart Grid Security

The data transmission of unencrypted information about customers' personal and location information threatens the customers' privacy [14], such as middle man attacks can change information in order to control price billing information. Smart grids consist of a network of sensors, monitors, Application devices, as well as data collection and analysis. All of these are susceptible to cyber-attacks, In real-time. Most of the available solutions neglect the security of data transmission when communicating information to and from the Smart Grid. More effort is required to ensure secure, reliable data transmissions among the various entities of the EV's management system.Smart Grid and fleet management systems exchange a large quantity of information, such as charging station load, electric vehicle battery states, traffic information, and unexpected events and accidents in the Smart Grid, electric cars, and charging stations. Any security attack may affect the ISO operation of the Smart Grid, the charging stations, and electric cars. For example, false infication and alteration of voltage or current level information may burn the electronic components in both electric vehicles and charging stations. Likewise.

## IV. Hackers Crash Concerns

Security information is necessary for the utility for billing, demand response, and load forecasting. The same information, however, can reveal the lifestyle of an individual. Each appliance has a unique electricity usage signature which can be extracted from the overall usage pattern indicating what the user is engaged in, i.e. working on a computer, criminals, can exploit this information for different purposes. Marketing companies could use this information for targeted marketing or intro- during non-competitive pricing. E- Criminals can be used this information to determine the daily routine or a family, i.e. when there is no one in the house or when someone is alone in the house for committing burglary or other crimes. Electricity theft can occur by altering the meter reading either by tampering with the meter or changing the information after breaking the encryption key [9]. There are several threats that the smart grid faces apart from dedicated attacks and intrusion by third parties [9–14], including privacy breach through data theft, electricity theft, disruption of services, physical damage to devices, denial of their- vice, and market fraud. Hacking into smart meters, tapping wireless communication, or stealing the data from servers of the utility can provide fine-grained metering information of the users' consumption [9]. Cyber –attacks on charging stations have identified five major challenges faced by computerised security systems related to smart grids [7] including a high volume of a sensitive customer of Information, distributed control devices, lack of physical protection, weak industry standards, and a large number of infected stakeholders dependent on the grid. The concerns of smart grid security as with other typical systems are confidentiality, integrity, and availability. Confidentiality entails protecting both consumer and operations data; integrity is also required both at the consumer level for metering and billing and at the operational level to ensure the stability of the grid; availability means that the power continues to be transmitted and received by customers, regardless of the status of the system. Smart grid faces the same security challenges as any complex computer network and needs both perimeter defence and visibility into the network. The fundamental issue of Hackers is that given massive size and interconnectivity in the entire network, worms and viruses can spread quickly. Also, given the distributed nature of the network, there are an enormous number of vulnerable targets such as Administrative passwords are often preceded and never changed from the original settings. There are several entry points into the networks. Additionally, SCADA systems are designed with inadequate security; for instance, Siemens still uses a hard-coded password for allowing access to control systems [8], which once compromised can lead to massive security breaches. Including infiltration through infected devices, network-based intrusion, compromised supply chain, and malicious insider.

## V. Charging Stations Vs Vulnerabilities

The network diagnostic of EV is more complex and vulnerable to different types of attacks. Smart grid network introduces enhancements and improved capabilities of the conventional power. Those attackers might falsely transmit to access charging stations as Vulnerabilities on the EVSEs network.

Table I: Vulnerabilities Charge Station

| | | |
|---|---|---|
| *1* | *Customer security* | Smart meters are collected huge data and transmit it to company, consumer and supportive information |
| *2* | *Greater number of intelligent devices* | Smart grid extremely has multi-intelligent components that are required manageable demand of electricity and network A moreover the smart grid network estimated 100 to 1000 times more than internet network. |
| *3* | *Physical security* | It is easy to insecure smart grid components unlike traditional power is had limited devices so increases vulnerabilities to physical access |
| 4 | *The lifetime of DC power systems* | Since power systems coexist with the relatively short-lived IT systems, it is inevitable that outdated equipment are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices. |
| 5 | *Implicit trust between traditional power devices* | State of false sending is considering vulnerable to data spoofing. So one device impacts another device or unwelcome device communication |
| 6 | *Different Team's backgrounds* | Vulnerability comes by bad Inefficient communication between teams |
| 7 | *Using Internet Protocol* | Attacker- based of the protocol as IP spoofing, IP Tear Drop and denial service IP. The advantage of using IP provides United among the components , however, if IP had attacked, all is damage |

## VI. Threats And Vulnerabilities Inside Charging Station Meters

There is no single device or mechanism that can provide all the necessary security measures required for cyber security of charge station or charge point. For improving the performance of DC power grid and changing the lives of electricity consumers As meters are the key components in smart grid infrastructure, smart meters accommodate the most valuable data (e.g. Meter readings and checks). For instance, meter readings are required to support many smart grid applications and services, including automatic meter reading, billing, dynamic pricing, and detection of impending blackouts and energy thefts, which can bring great convenience to both utilities and energy consumers. However, the massive amount of data collected from smart meters should be carefully protected against misuse. It is desirable to incorporate security mechanisms into the design and implementation of the smart meter infra- structure so as to increase robustness and resilience for the system and gain energy consumers' trust.Skopik et al. [12] analysed the security threats and vulnerabilities in smart meter infrastructure detailed in three tiers: smart meters, utility, and Web application. The first-tier smart meter vulnerabilities are categorised as the attacks to the smart grid. ID customer, EV's location, time and data of running, plate of EV are factors to effect next charging stations . in deep meaning, if one of those is attacked, all considers damage calculation However, the meter reading is uncertainty to consume electricity correctly. These may also include inquiries, alarms, or Notifications. Effects system stability and reliability and also safety Configuration Data Configuration data (system operational settings and security credentials, also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may play to be updated power system stability and safety Time, Clock Setting Time is used in records sent to other entities. Phase or measurement directly relates to controlling system actions. Moreover, time is also needed to use tariff information optimally. It may also be used in certain security protocols Determination whether a communication peer is entitled to send and receive commands and data. Such policies may consist of lists of Effects system control system stability, reliability, and their credentials, and their roles. The car manufacturer, Their correctness is critical markets for the energy system providers may inform consumers of new or temporary tax as a base of the final decision of customers privacy through competitions.

## VII. Charger Poles Attack And Types Of Attacks

Charge poles The Attacks are remembered vulnerability may be operated by attackers with various ideas and could cause different damage to the network. Attackers do not distinguish different motives among employees and customers. So that the authors has tried categorised group of attackers like

1. non- malicious attackers who informed us the security operation system into confusing and puzzle, those have strong desire to destroy IOP but the curiosity is intellectual challenge
2. revenge is driven consumers against others to shut down the powers, and it is impossible to figure out their problems.
3. In more visible events in nowadays, terrorists who specify the smart grid is attractive goal to impact million of people
4. The financial purpose of consumers is illustrated attacking each other's[5],[6], the wide variety of attacks is classified Component –wise is Remote Terminal Unit(RTU) target that is interested in engineers who solve troubleshoot on the smart grid devices so, malicious users blamed issues fault which is caused shutting down, protocol- wise is protocol attacker itself that is murder as reversal decision can be false date infection . topology- wise has great power and includes Denial of service attacking that keeps power operation of having full charging.

Those are more dangerous attackers as [7],[10].

1. Malware Spreading which is to infect smart meters and wireless services, it is suicide attacker that replace some functions or add false date
2. Access during database links: control system still lives database and record its own activities, however to access of skilled attacker may exploit weak database management on the system network.
3. Communicative equipment compromising:
   multiplexers consider communication device that works direct danger as a backdoor to forecast future threatening.
4. false information is injecting : to inject false prices, fake data of meters can be caused a huge financial impact on the electricity markets. [19]
5. network capacity: Vulnerabilities are tried to used IP protocol and TCP/IP to become easer target so that DOS attacks can corrupt information carrying in order to delay figure out smart grid problems.
6. Eavesdropping and traffic analysis the mentor of network traffic has been sensitive transportations that consist billing information, wireless infrastructure and attackers curiosity.
7. Modbus Security Issue: Modbus protocol is one piece of the SCADA system The term SCADA refers to computer systems and protocols that track the monitor [18]
   And control industrial, infrastructure, or facility-based processes such as smart grid processes.it is responsible for exchanging SCADA information needed to control industrial processes. Given that the Modbus protocol was not designed for highly security-critical environments, several attacks are possible including: (a) sending fake broadcast messages to slave devices (Broadcast message spoofing), (b) replaying genuine recorded messages back to the master (Baseline response replay), (c) locking out a master and controlling one or more field devices (Direct slave control), (d) sending benign messages to all possible addresses to collect devices' information (Modbus network scanning), (e) reading Modbus messages (Passive reconnaissance), (f) delaying response messages intended for the masters (Response delay), and (g) attacking a computer with the appropriate adapters (Rouge interloper)[19].

## VIII. Conclusion

The technology of charging station makes it an easy target for attackers. In particular, cascaded attacks and worm infections can propagate faster than other components. This article introduces the research situation and research achievements on a related demonstrative project in detail, Electric vehicle equipment and technology are one of the loads that carry a high risk of security. Cybersecurity is a growing concern and is very important and critical for a successful deployment of a smart grid system The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber-attacks. Electric vehicle charging station system under the condition of Smart Grid discusses the key technologies of electric vehicle charging station and indicate a cyber attack. Charge station is one of the critical components for the development of electric vehicle charging station. Electric vehicle charging station technology can promote smart grid security, accord with current energy utilisation patterns of energy conservation. Because the smart grid is vulnerable due to having a massive number of Attackers may compromise loads, smart meters, transmission and distribution equipment, PMUs, sensors, computers and so on. We reviewed the cyber - attackers issues for charge station in the smart grid. Since the smart grid technology is considered a critical infrastructure, An enterprise undertaking a charge station project need to work closely with the smart grid system. All vulnerabilities should be identified and figure out sufficient solutions onto the smart grid.

## REFERENCES

[1] Arman, N. A., Logenthiran, T., & Woo, W. L. (2015). Intelligent energy management of distributed energy storage systems in the microgrid. 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA). doi:10.1109/isgt-asia.2015.7387076 http://dx.doi.org/10.1109/ISGT-Asia.2015.7387076

[2] Bhagyashree Patil, & Maruti Limkar. (2015). Machine To Machine Communication Based Smart Metering System. IJERT, V4(06). doi:10.17577/ijertv4is060396 http://dx.doi.org/10.17577/IJERTV4IS060396

[3] Bhatti, A. R., Salam, Z., Aziz, M. J., Yee, K. P., & Ashique, R. H. (2016). Electric vehicles charging using photovoltaic: Status and technological review. Renewable and Sustainable Energy Reviews, 54, 34-47. doi:10.1016/j.rser.2015.09.091 http://dx.doi.org/10.1016/j.rser.2015.09.091

[4] Collins, L. (2014). Securing the Infrastructure. Cyber Security and IT Infrastructure Protection, 247-267. doi:10.1016/b978-0-12-416681-3.00010-0 http://dx.doi.org/10.1016/B978-0-12-416681-3.00010-0

[5] Communication Reduced Interaction Protocol between Customer, Charging Station, and Charging Station Management System. (2014). Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems. doi:10.5220/0004971801180125 http://dx.doi.org/10.5220/0004971801180125

[6] Deng, B., & Wang, Z. (2011). Research on Electric-Vehicle Charging Station Technologies Based on Smart Grid. 2011 Asia-Pacific Power and Energy Engineering Conference. doi:10.1109/appeec.2011.5748759 http://dx.doi.org/10.1109/APPEEC.2011.5748759

[7] Elliman, R., Gould, C., & Al-Tai, M. (2015). Review of current and future electrical energy storage devices. 2015 50th International Universities Power Engineering Conference (UPEC). doi:10.1109/upec.2015.7339795 http://dx.doi.org/10.1109/UPEC.2015.7339795

[8] International Conference On Transportation Engineering (5th : 2015 : Dalian, China). (2015).ICTE 2015: Proceedings of the Fifth International Conference on Transportation Engineering : September 26-27, 2015, Dalian, China.

[9] Leviton Evr-Green Electric Vehicle Charging Stations. (n.d.). Retrieved from http://www.leviton.com/OA_HTML/SectionDisplay.jsp?section=37818&minisite=10251

[10] Li, H., Sun, G. M., & Chu, Y. (2012). Design of Integrated Monitoring System for Electric Vehicle Charging Station Based on Weblogic. AMM, 241-244, 2004-2009. doi:10.4028/www.scientific.net/amm.241-244.2004 http://dx.doi.org/10.4028/www.scientific.net/AMM.241-244.2004

[11] Marcincin, O., & Medvec, Z. (2015). Active charging stations for electric cars. 2015 16th International Scientific Conference on Electric Power Engineering (EPE). doi:10.1109/epe.2015.7161084 http://dx.doi.org/10.1109/EPE.2015.7161084

[12] Mousavian, S., Erol-Kantarci, M., & Ortmeyer, T. (2015). Cyber Attack Protection for a Resilient Electric Vehicle Infrastructure. 2015 IEEE Globecom Workshops (GC Wkshps). doi:10.1109/glocomw.2015.7414174 http://dx.doi.org/10.1109/GLOCOMW.2015.7414174

[13] Nie, X., Liu, J., Xuan, L., Liang, H., Pu, S., Wang, Q., & Zhou, N. (2013). Online monitoring and integrated analysis system for EV charging station. 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC). doi:10.1109/appeec.2013.6837206 http://dx.doi.org/10.1109/APPEEC.2013.6837206

[14] Singh, M., Kumar, P., & Kar, I. (2012). A model of Electric Vehicle charging station compatibles with Vehicle to Grid scenario. 2012 IEEE International Electric Vehicle Conference. doi:10.1109/ievc.2012.6183223 http://dx.doi.org/10.1109/IEVC.2012.6183223

[15] Ma, C., Rautiainen, J., Dahlhaus, D., Lakshman, A., Toebermann, J. C., & Braun, M. (2015). Online Optimal Charging Strategy for Electric Vehicles.Energy Procedia, 73, 173-181. http://dx.doi.org/10.1016/j.egypro.2015.07.667

[16] Falk, R., & Fries, S. (2012). Electric Vehicle Charging Infrastructure Security Considerations and Approaches. Proc. of INTERNET, 58-64.

[17] http://www.chargepoint.com/ access 25-07-2016

[18] Yuvaraj S. Patil Dr. Mrs. Swati V. Sankpal, May 15 Volume 3 Issue 5, "A Survey on Cyber Security for Smart Grid Networks", International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 2503 - 2507, DOI:10.17762/ijritcc2321-8169.150502

[19] Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*, 1-6. doi:10.12720/sgce.1.1.1-6 http://dx.doi.org/10.12720/sgce.1.1.1-6

S.AHMED received the M.S. degree incomputer science from UUM University utrla Malaysia (UUM), Malaysia, in 2008. He is currently Assistant Lecturer. His research interests include renewable energy, electric vehicle,ICT.

F. M. Dow received the B.S. degree from the Department of electric engineering , Sart University, Libya, in 2003, and the M.S.degrees in electric engineering from Libyan academic in 2013 .He is currently working Libyan Authority for research, science and technology. His research interests include the smart grid and renewable energy.

.