ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Addressing Security in OCPP: Protection against Man-in-the-Middle Attacks

M.Manivel, P.Pukazhmani, R.Kowsalya, S.Muthusamy,

UG Scholar, Dept. of CSE, Surya Engineering College, Erode, Tamilnadu, India

UG Scholar, Dept. of CSE, Surya Engineering College, Erode, Tamilnadu, India

UG Scholar, Dept. of CSE, Surya Engineering College, Erode, Tamilnadu, India

Assistant Professor, Dept. of CSE, Surya Engineering College, Erode, Tamilnadu, India

ABSTRACT: The Open Charge Point Protocol (OCPP) is a communication standard for theexchange of data between a Charge Point (CP) and the Central Server (CS) in theelectric vehicle domain. This protocol is envisioned to offer interoperability betweenthe different manufacturers of charging points, network systems and IT back-end vendors. However, the current version of the specification is quite vague in terms of handling security and privacy, which results in a set of non-addressed threats, which we look at in this paper. Specifically, this paper focuses on Man-in-the-Middle attacks between the CP and the CS that may expose sensitive data of special interest to the various stakeholders involved in this context. As a counter-measure, we present a feasible solution and assess its behaviour in a simulator. The inclusion of additional security mechanisms is also studied, in compliance with the IEC 62351 standard.

I. INTRODUCTION

LOCATION awareness has become an asset in mobile systems, where a wide range of protocols and applications require knowledge of the position of the participating nodes. Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information. The correctness of node locations is therefore an allimportant issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In these cases, we need solutions that let nodes 1) correctly establish their location in spite of attacks feeding false location information, and 2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations. In this paper, we focus on the latter aspect, hereinafter referred to as neighbor position verification (NPV for short). Specifically, we deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. For example, by advertising forged positions, adversaries could bias geographic routing or data gathering processes, attracting network traffic and then eavesdropping or discarding it. Similarly, counterfeit positions could grant adversaries unauthorized access to location- dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers. In this context, the challenge is to perform, in absence of trusted nodes, a fully distributed, lightweight NPV procedure that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. We therefore propose an NPV protocol that has the following features: . It is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes; . It leverages cooperation but allows a node to perform all verification procedures autonomously. This approach has no need for lengthy interactions, e.g., to reach a consensus among multiple nodes, making our scheme suitable for both low- and highmobility environments; . It is reactive, meaning that it can be executed by any node, at any point in time, without prior knowledge of the neighborhood; . It is robust against independent and colluding adversaries; . It is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

lightweight, as it generates low overhead traffic. Additionally, our NPV scheme is compatible with state-ofthe- art security architectures, including the ones that have been proposed for vehicular networks, which represent a likely deployment environment for NPV.

Objectives:

We have designed an approach that preserves the privacy when sending smart meters data in OCPP, which has been validated by means of a test case in a simulator, as described in Section

II. EXISTING SYSTEM

- Smart Grid technologies offer multiple improvements over the traditional grid model, due to the real-time communication between smart meters on the customer's premises and the supervision systems of the central stationdoes not specify any underlying communication technology (e.g., Power Line Communication) and does not define strong security services .
- This means it relies on the security provided by other protocols at lower levels. In the current version of the specification version 1.6, released in (version 2.0 is under development),suggests the use of Transport Layer Security (TLS) at the transport layer to provide confidentiality for communication links.
- However, this protocol has been demonstrated to be insecure against Man-in-the-Middle (MITM) attacks in certain scenarios, especially in the EV context where it is difficult to guarantee true end-to-end security. This is because, on the one hand, TLS is vulnerable with respect to certificates validation which can lead to communication hijacking

III. PROPOSED SYSTEM

- In this study, we describe a technique that enables the transmission of the energy values securely, so only CP and CS know the actual energy usage data, proposing a solution for future versions of the standard. In order to provide confidentiality to this communication.
- we use the Data Transfer operation defined in OCPP, that allows both the CP and CS to send generic information to each other, so additional functions not defined in OCPP can be flexibly implemented. For our particular purpose, we have designed a light modification of the original charge operation to include an additional step after the StopTransaction request, where the meterStop is sent securely by applying different cryptographic mechanisms.
- This solution is based on a secret sharing scheme, which provides a robust measure against MITM attacks, and is simulated and analysed.
- When focusing on the OCPP scenario, this algorithm becomes even more useful. Let us assume a situation in which EV users perform several charges on the CP over given a time period. Each transaction consequently generates a meter value that must be dispatched to the CS to carry out billing and demand response. In accordance with the proposed scheme, that data is sent in the form of shares over multiple, separate transmissions.

Modules:

- Node creation.
- Discover Neighbor Node's
- Verify Neighbor Node's Position.
- Find out the adversarial nodes.

Node Creation:

- In this module, we create Nodes and form a Network.
- Users enter the Node Name, IpAddress, port number, of the node to register in the Database.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

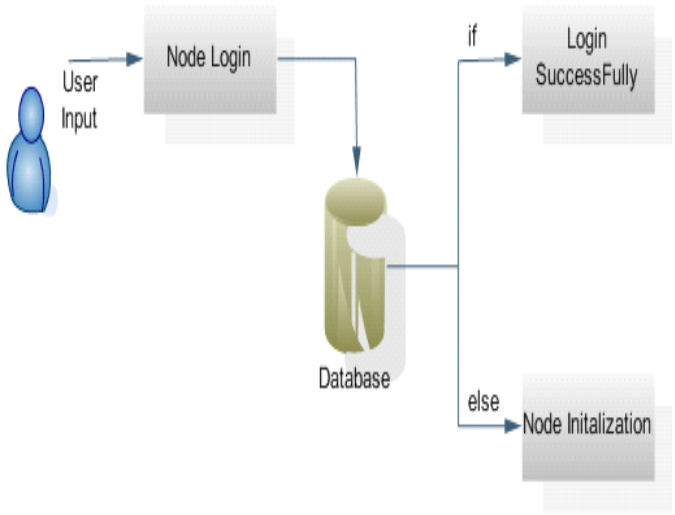
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

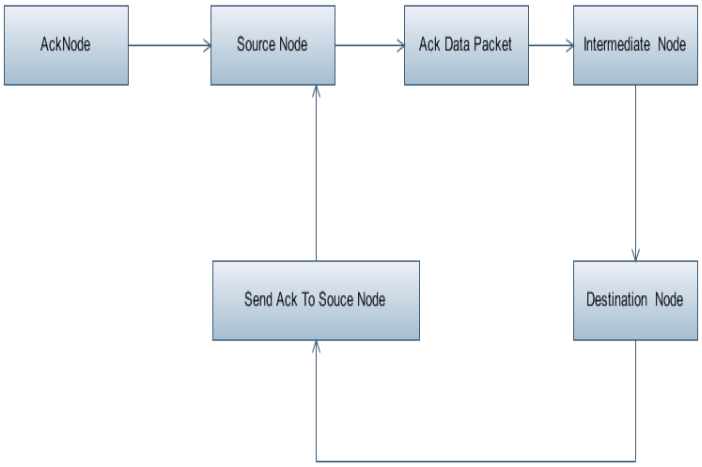
Vol. 8, Issue 3, March 2019

- While entering the next node the user must check the database for that node exists or new one.



Ack:

- In this acknowledgement mode to select the source node then send the Ack Data Packet through the intermediate node to verify the data then destination node.
- The destination node to receive the data then back to send ack to the source node.
- .In this ACK node, node S first sends out an ACK data packet *Pad*1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order.
- Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful.
- Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

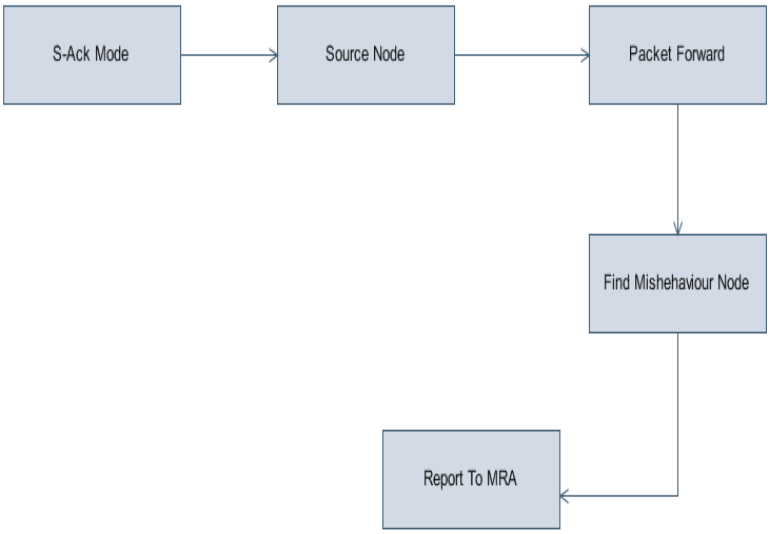
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

S-Ack:

- In this mode source node packet are forward to the destination. it can find the misbehave node then send report to MRA.
- The S-Ack Mode consecutive three nodes work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *Psad*1 to node F2. Then, node F2 forwards this packet to node F3.
- When node F3 receives *Psad*1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 forwards *Psak*1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious.



MRA:

- To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node.

- The destination has the packet the report as trust the packet are correct and another way mark report as malicious then send Ack Packet to the Source node.

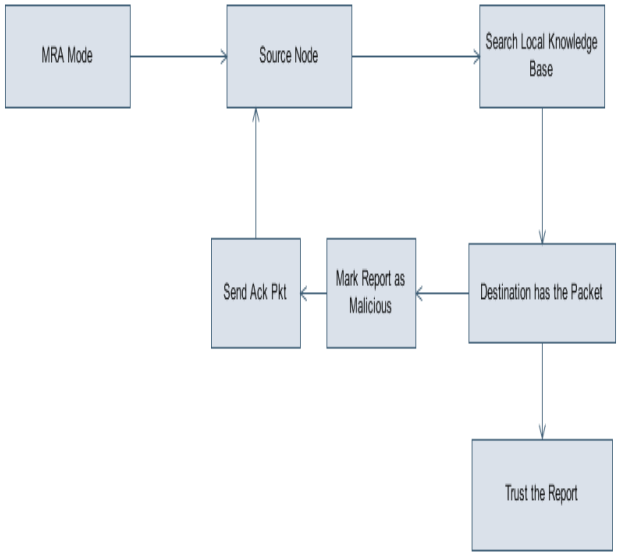
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

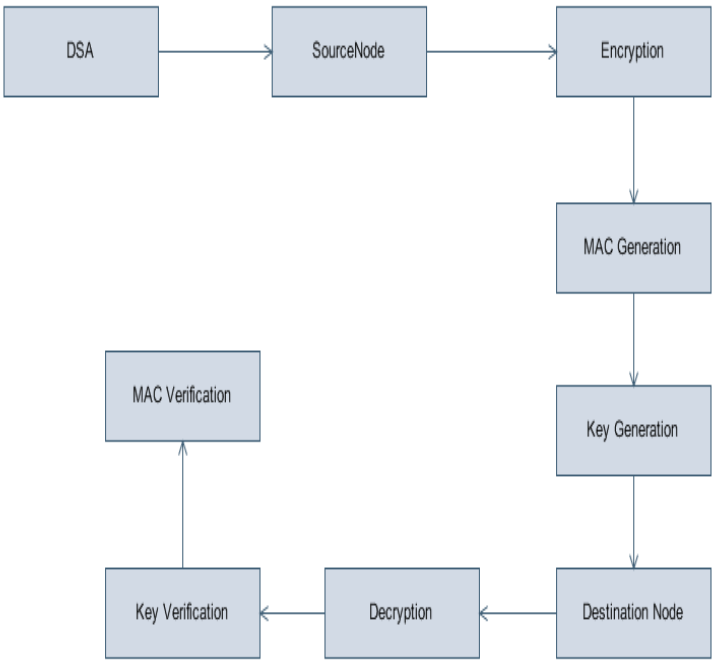
Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019



DSA:

- The DSA source node data are encrypted and MAC and Key generation to the destination and target node decrypt the content and verify the MAC and Key.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

IV. FUTURE ENHANCEMENT

- Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
- Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys;

V. CONCLUSION

We presented a distributed solution for Position, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier. Simulation results confirm that our solution is effective in identifying nodes advertising false positions, while keeping the probability of false positives low. Only an overwhelming presence of colluding adversaries in the neighborhood of the verifier, or the unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NPV. Future work will aim at integrating the NPV protocol in higher layer protocols, as well as at extending it to a proactive paradigm, useful in presence of applications that need each node to constantly verify the position of its neighbors.

REFERENCES

[1] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.
[2] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[3] M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos, "Secure Neighbor Position Discovery in Vehicular Networks," Proc. IEEE/IFIP 10th Ann. Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), June 2011.
[4] PRECIOSA: Privacy Enabled Capability in Co-Operative Systems and Safety Applications, http://www.preciosa-project.org, 2012.
[5] J. Ha¨rri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation with VanetMobiSim," Trans. Soc. Modeling & Simulation, 2009.