

INTELLIGENT AUTHENTICATION SYSTEM FOR LOAD MANAGEMENT

Dr.T.R.Rangaswamy¹, Dr.V.Jayalakshmi²

Professor^{1,2}, Department of EEE, BIST, BIHER, Bharath University, Chennai.

rangaswamy.eee@bharathuniv.ac.in

ABSTRACT

In Smart Grid, the demand management consist of the planning, implementing, and monitoring activities of electric utilities. Load dispatch centre is playing major role by matching the power demand with system integrity, reliability and security of generation and transmission facilities. It also regulates the grid frequency to balance the demand and the generation of power with optimum utilization of resources. To control the frequency the load despatch centres communicate with other power plants through communication network. The data communication should be well secured.

In this paper a security system is proposed using intelligent authentication code, to avoid participation of unauthorized person with an intension of creating attacks. Load dispatch centre generates dynamic secret authentication code at the end of each communication to power plants.

When the load dispatch centre is sending data (instruction) to power plant, it uses a secret code. The secret code vary from one power plant to another power plant. The code is known only by the load dispatch centre and the respective power plant. After carrying out the assignment, the power plant acknowledge the load dispatch centre. Finally the load dispatch centre generates new code and send to power plant. Load dispatch centre and power plants should store the last communicated code to utilize for next communication. Either load dispatch centre or power plant wanted further communication, they should compare and use

the code which was stored at the end of lost conversation.

The scheme is simulated using HTML and PHP. The simulation result proves that the proposed scheme is suitable for blocking unauthorised entry[1-5]. The scheme is protected from spoofing, dictionary attack, sniffing and man in the middle attack.

I. INTRODUCTION

Load dispatch centre is an important link between generation and transmission stations. Load despatch centre is characterized by two-way communication between the sub-stations and generating stations. The load dispatch centre monitor supervise and control the grid system[6-11]. It provides integrity, reliability and security of generation and transmission facilities. Also carry out scheduling and dispatch of load within the region.

It maintains system frequency almost between 49.5 Hzs to 50.5 Hzs range by regulating the generation Load as per the demand. Communication between load dispatch centre and the generation station should maintain confidentiality and integrity through message authentication code (MAC) services.

Attila Altay Yavuz, [12-17] developed a Rapid Authentication (RA) method followed to command and control messages in large and distributed systems. In this scheme there is fast signature generation and verification, constant size public key, highly secured without time synchronization requirement were developed. Mostafa M. Fouda et al[2] proposed a lightweight message

authentication scheme features as a basic yet crucial component for secure communication framework. Specifically, in the proposed scheme, the smart meters which are distributed at different hierarchical networks can first achieve mutual authentication and establish the shared session key with Diffie-Hellman exchange protocol. Then, with the shared session key between smart meters and hash-based authentication code technique, the subsequent messages can be authenticated in a lightweight way. Yining Liu et al [18-23] proposed a lightweight authenticated communication scheme for the smart grid, which ensures a secure two-way communication between the smart meters and the neighbourhood gateway and carried out security analysis. Göran N .Ericsson [24] discussed cyber security issues, and it highlighted the access points in a substation. Also, information security domain modeling was treated. Velin Kounev et al [25] proposed secure communication architecture to support microgrid operation and control. A security model, including network, data, and attack models, was defined and a security protocol to address the real-time communication needs of microgrids. Yutaro Yamaguchi et al [26] presented exact solution methods for analysing vulnerability of electric power networks to a certain kind of undetectable attacks known as false data injection attacks. They have shown that the problems of finding the minimum number of measurement points to be attacked undetectably reduce to minimum cut problems on hypergraphs, which admit efficient combinatorial algorithms. Danda Betal [27] et al. investigated Chi-square detector and cosine similarity matching approaches for attack detection in smart grids where Kalman filter estimation was used to measure any deviation from actual measurements. The cosine similarity

matching approach is found to be robust for detecting false data injection attacks as well as other attacks in the smart grids. Once the attack is detected, system can take preventive action and alarm the manager to take preventative action to limit the risk. Kebina Manandhar et al [28] presented a mathematical model of the system to study these pitfalls and propose a robust security framework for the smart grid. The framework adopts the Kalman filter to estimate the variables of a wide range of state processes in the model. The estimates from the Kalman filter and the system readings are then fed into the χ^2 -detector or the proposed Euclidean detector [29-33]. The χ^2 -detector is a proven effective exploratory method used with the Kalman filter for the measurement of the relationship between dependent variables and a series of predictor variables. The χ^2 -detector can detect system faults/attacks, such as DoS attack, short-term, and long-term random attacks. Jiankun Hu, et al [9], surveyed and discuss new findings and developments in the existing big energy data analytics and security. Several taxonomies have been proposed to express the intriguing relationships of various variables in the field. Bin Hu et al [34-40], introduced a dynamically updating key distribution strategy to enhance mesh network security against cyber attack. The scheme has been applied to two security protocols known as simultaneous authentication of equals (SAE) and efficient mesh security association (EMSA). Since both protocols utilize 4-way handshaking, they proposed a Merkle-tree based handshaking scheme, which is capable of improving the resiliency of the network in a situation where an intruder carries a denial of service attack. Finally, by developing a denial of service attack model, they evaluated the security of the proposed schemes against

cyber attack, as well as network performance in terms of delay and overhead.

The load dispatch centre offers secure and intelligent load distribution from power plants using communication technologies to control the demand. Increased interconnectivity of power plants with load dispatch centre over the grid systems generate new challenges for security and its management.

On order to give more importance to the security, an Intelligent message authentication code is proposed in this paper.

This paper is organized as follows: Section 1 presents the introduction and the prose of the previous research, Section 2 describes existing method. Section 3 describes the proposed method. Section 4 describes implementation of the scheme and Section 5 deals with results & conclusion[41-45].

2. Existing system

The message from LDC goes through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the power plant. The power plant in turn runs the message through the same MAC algorithm using the same key, producing a second MAC data tag. The power plant then compares the first MAC tag received in the transmission to the second generated MAC tag.

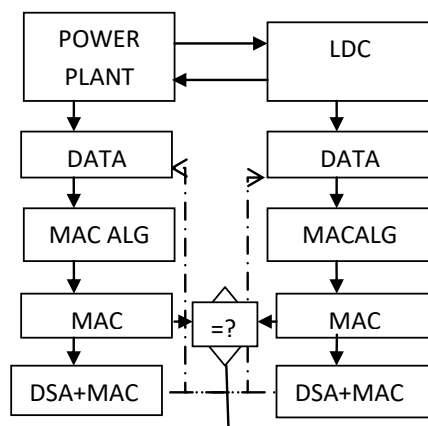


Fig. 1. The existing authentication system

The block diagram of the existing system is shown in Fig.1.

If they are identical, the power plant can safely assume that message was not changed by any attacker during transmission. Same procedure is followed whenever data communicated from power plant to Load centre.

3. THE PROPOSED SYSTEM

The load despatch centre communicates with several power plants. The confidentiality of data is to be maintained and the data communication must be in a secured manner.

Authentication is concerned with protecting the integrity of a message and validating identity of originator.

When the load despatch centre is sending data (instruction) to power plant, the load despatch centre uses a secret code. The secret code vary from one power plant to another power plant. The code is known only by the load despatch centre and the respective power plant. General communication network is shown in Fig.2.

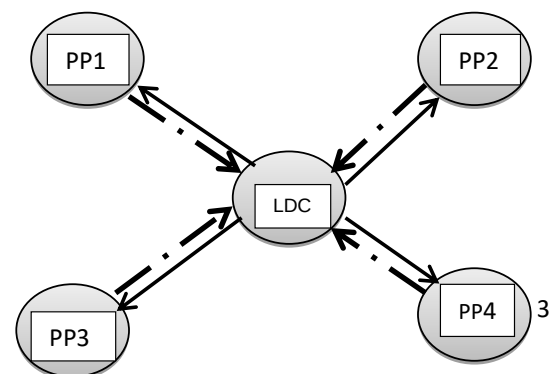


Fig.2. Communication network of LDC & PP

The communication block diagram between load dispatch centre (LDC) & Power plant (PP) is shown in Fig.3. For example, (shown in Fig.2) when the load dispatch server required to instruct the power plant to increase the load to 30MW, it sends a message "INCREASE 30 MW" with a secret code attached before and after the message as "AA INCREASE 30 MW BB".

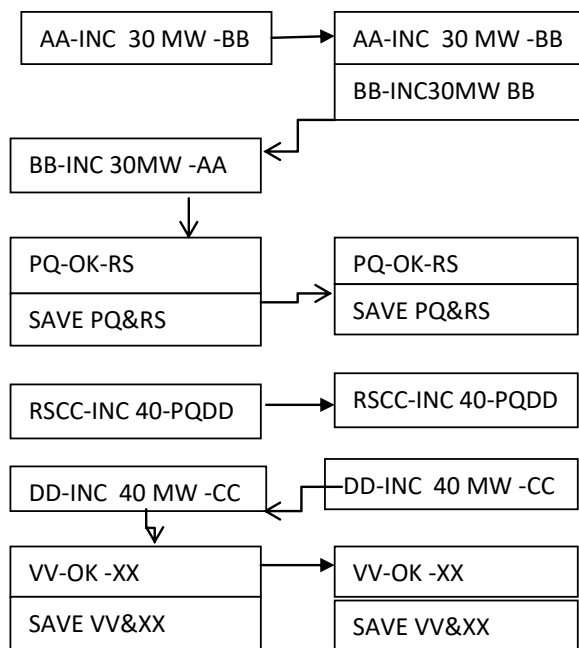


Fig.3. Communication between LDC & PP

The power plant (receiver server) receives message and reply new the message to load dispatch center (sender) with secret key in a reversed order as "BB INCREASE 30 MW" AA. The load dispatch centre (sender) identifies the authenticity of

message received and send "ok" message with secret code attached before and after as "PQ OK RS" to power plant. The power plant increases the load to 30 MW. Also the power ant and LDC saves the last transaction code for future communication. ("PQ OK RS")

After some time delay, if the LDC required to send data to Power plant uses the previously saved secret code, (PQCC INCREASE 40MW RSDD) then Power plant compares the last corresponded secret code and send reply to LDC ,(DDRS INCREASE 40MW CCPQ)

LDC identifies the correct message received by the power plant and send a newly generated code to power plant (VV OK WW). This new code will be saved for the next communication by both LDC and PP.

This concept is to prove the authenticity of the intruder. It is an interactive method for one party to prove to another party (the verifier) for a validity. By implementing this concept, the hackers cannot get access to the data either from LDS or from Power plants.

4. Implementation Of Proposed Method

Implementation was carried out using HTML and PHP with a focus on high security. When a message is sent by load dispatch centre, an application program will generate an authentication adder in the form of secret code, mathematical manipulation, graphics etc

Data base "msgdb" was created in php MyAdmin as shown in Fig 4

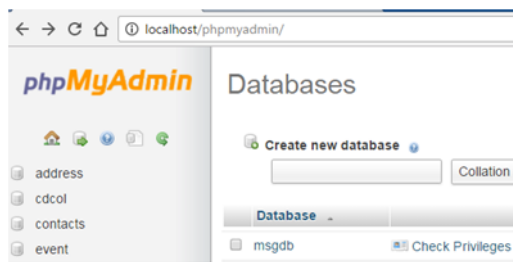


Fig 4. Creation of new data base msgdb

Table was created to save the communication in the database as shown in Fig. 5.

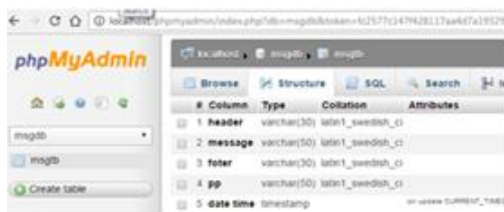


Fig.5. Table creation for database

The LDC starts communication with PP using authentication code as shown in Fig.6. The load dispatch sends instruction using authentication code will be verified by the power plants. Same way, when Power plants sends the data with authentication code to the load dispatch will be verified by the LDC.

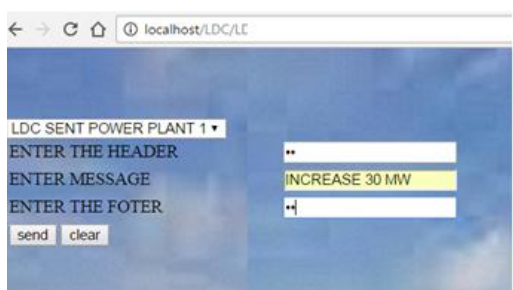


Fig.6. Communication with secret code.

After completing the authentication process, Power plants will carry out the instruction and gives acknowledgement with new authentication code to the load dispatch. New

authentication code will be stored with time stamp and will be used in the next transaction by both LDC & PP.

Each communication between power plant and load dispatch centre is stored in the data base for verification as shown in Fig. 7.

header	message	foter	pp	date time
aa	INCREASE 30 MW	bb	LDC SENT POWER PLANT 1	2017-02-04 15:33:12
BB	INCREASE 30 MW	AA	POWER PLANT 1 SENT TO LDC	2017-02-04 15:54:17
pq	ok	rs	LDC SENT POWER PLANT 1	2017-02-04 16:23:27
cc	INCREASE 30 MW	dd	LDC SENT POWER PLANT 1	2017-02-06 11:27:54

Fig.7. Event recording

If any unauthorized person sends instruction without proper authentication code will not be accepted and the error message will be displayed as shown in Fig. 8.

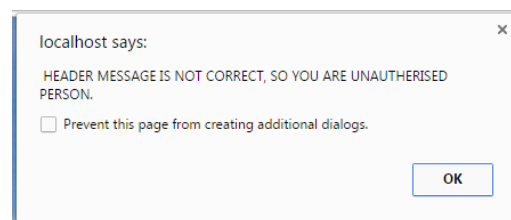


Fig.8. Error Message for attackers.

5. Conclusions

The intelligent MAC system gives efficient security solution to protect from attackers. The authentication system is made dynamic. When the power plant gets the message with secret code, an application program calls verification service and verifies the code by comparing it with the code received during the last message. If the two codes are the same, further processing will be continued otherwise the communication will be rejected with a warning message.

This protocol is an interactive method to verify the intelligent code for the authentication of the load dispatch centre and the power plants. So the hackers are not able to respond to the conversations initiated by the server. The data

transmitted over the transaction is not usable by the hacker to fake an identity. The use of secret code sent and receive is only valid once and within a time limit. Thus, it will not be usable by attackers who intercept the information. Intruder if any cannot be interacted easily

The communications are protected from spoofing, dictionary attack, credential stealing attack, sniffing and man in the middle attack.

REFERENCES

1. Nimal, R.J.G.R., Hussain, J.H., Effect of deep cryogenic treatment on EN24 steel, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-113-116, 2017
2. Parameswari, D., Khanaa, V., Deploying lamport clocks and linked lists, International Journal of Pharmacy and Technology, V-8, I-3, PP-17039-17044, 2016
3. Parameswari, D., Khanaa, V., Case for massive multiplayer online role-playing games, International Journal of Pharmacy and Technology, V-8, I-3, PP-17404-17409, 2016
4. Parameswari, D., Khanaa, V., Deconstructing model checking with hueddot, International Journal of Pharmacy and Technology, V-8, I-3, PP-17370-17375, 2016
5. Parameswari, D., Khanaa, V., The effect of self-learning epistemologies on theory, International Journal of Pharmacy and Technology, V-8, I-3, PP-17314-17320, 2016
6. Pavithra, J., Peter, M., GowthamAashirwad, K., A study on business process in IT and systems through extranet, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-571-576, 2017
7. Pavithra, J., Ramamoorthy, R., Satyapira Das, S., A report on evaluating the effectiveness of working capital management in googolsoft technologies, Chennai, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-129-132, 2017
8. Pavithra, J., Thooyamani, K.P., A cram on consumer behaviour on Mahindra two wheelers in Chennai, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-55-57, 2017
9. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the air freight customer satisfaction, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-179-184, 2017
10. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the working capital management of TVS credit services limited, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-185-187, 2017
11. Pavithra, J., Thooyamani, K.P., Dkhar, K., A study on the analysis of financial performance with reference to Jeppiaar Cements Pvt Ltd, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-189-194, 2017
12. Peter, M., Dayakar, P., Gupta, C., A study on employee motivation at Banalari World Cars Pvt Ltd Shillong, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-291-294, 2017
13. Peter, M., Kausalya, R., A study on capital budgeting with reference to signware technologies, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-71-74, 2017
14. Peter, M., Kausalya, R., Akash, R., A study on career development with reference to premheerasurgicals, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-415-420, 2017
15. Peter, M., Kausalya, R., Mohanta, S., A study on awareness about the cost reduction and elimination of waste among employees in life line multispeciality hospital, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-287-293, 2017
16. Peter, M., Srinivasan, V., Vignesh, A., A study on working capital management at deccan Finance Pvt Limited Chennai, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-255-260, 2017
17. Peter, M., Thooyamani, K.P., Srinivasan, V., A study on performance of the commodity market based on technicalanalysis, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-99-103, 2017
18. Philomina, S., Karthik, B., Wi-Fi energy meter implementation using embedded linux in ARM 9, Middle - East Journal of Scientific Research, V-20, I-12, PP-2434-2438, 2014
19. Philomina, S., Subbulakshmi, K., Efficient wireless message transfer system, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-289-293, 2017

20. Philomina, S., Subbulakshmi, K., Ignition system for vehicles on the basis of GSM, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-283-286, 2017
21. Philomina, S., Subbulakshmi, K., Avoidance of fire accident by wireless sensor network, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-295-299, 2017
22. Pothumani, S., Anuradha, C., Monitoring android mobiles in an industry, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-537-540, 2017
23. Pothumani, S., Anuradha, C., Decoy method on various environments - A survey, International Journal of Pure and Applied Mathematics, V-116, I-10 Special Issue, PP-197-199, 2017
24. Pothumani, S., Anuradha, C., Priya, N., Study on apple iCloud, International Journal of Pure and Applied Mathematics, V-116, I-8 Special Issue, PP-389-391, 2017
25. Pothumani, S., Hameed Hussain, J., A novel economic framework for cloud and grid computing, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-5-8, 2017
26. Pothumani, S., Hameed Hussain, J., A novel method to manage network requirements, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-9-15, 2017
27. Pradeep, R., Vikram, C.J., Naveenchandra, P., Experimental evaluation and finite element analysis of composite leaf spring for automotive vehicle, Middle - East Journal of Scientific Research, V-12, I-12, PP-1750-1753, 2012
28. Prakash, S., Jayalakshmi, V., Power quality improvement using matrix converter, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-95-98, 2017
29. Prakash, S., Jayalakshmi, V., Power quality analysis & power system study in high voltage systems, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-47-52, 2017
30. Prakash, S., Sherine, S., Control of BLDC motor powered electric vehicle using indirect vector control and sliding mode observer, International Journal of Pure and Applied Mathematics, V-116, I-19 Special Issue, PP-295-299, 2017
31. Prakesh, S., Sherine, S., Forecasting methodologies of solar resource and PV power for smart grid energy management, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-313-317, 2017
32. Prasanna, D., Arulselvi, S., Decoupling smalltalk from rpcs in access points, International Journal of Pure and Applied Mathematics, V-116, I-16 Special Issue, PP-1-4, 2017
33. Prasanna, D., Arulselvi, S., Exploring gigabit switches and journaling file systems, International Journal of Pure and Applied Mathematics, V-116, I-16 Special Issue, PP-13-17, 2017
34. Prasanna, D., Arulselvi, S., Collaborative configurations for wireless sensor networks systems, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-577-581, 2017
35. Priya, N., Anuradha, C., Kavitha, R., Li-Fi science transmission of knowledge by way of light, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-285-290, 2017
36. Priya, N., Pothumani, S., Kavitha, R., Merging of e-commerce and e-market-a novel approach, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-313-316, 2017
37. Raj, R.M., Karthik, B., Effective demining based on statistical modeling for detecting thermal infrared, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-273-276, 2017
38. Raj, R.M., Karthik, B., Energy sag mitigation for chopper, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-267-270, 2017
39. Raj, R.M., Karthik, B., Efficient survey in CDMA system on the basis of error revealing, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-279-281, 2017
40. Rajasulochana, P., Krishnamoorthy, P., Ramesh Babu, P., Datta, R., Innovative business modeling towards sustainable E-Health applications, International Journal of Pharmacy and Technology, V-4, I-4, PP-4898-4904, 2012
41. Rama, A., Nalini, C., Shanthi, E., An iris based authentication system by eye localization, International Journal of Pharmacy and Technology, V-8, I-4, PP-23973-23980, 2016

42. Rama, A., Nalini, C., Shanthi, E., Effective collaborative target tracking in wireless sensor networks, International Journal of Pharmacy and Technology, V-8, I-4, PP-23981-23986, 2016
43. Ramamoorthy, R., Kanagasabai, V., Irshad Khan, S., Budget and budgetary control, International Journal of Pure and Applied Mathematics, V-116, I-20 Special Issue, PP-189-191, 2017
44. Ramamoorthy, R., Kanagasabai, V., Jivandan, S., A study on training and development process at Vantec Logistics India Pvt Ltd, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-201-207, 2017.
45. Pradeep, R., Vikram, C.J., Naveenchandran, P., Experimental evaluation and finite element analysis of composite leaf spring for automotive vehicle, Middle - East Journal of Scientific Research, V-17, I-12, PP-1760-1763, 2013

