www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 20134-20136
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.51

Survey on a Lightweight Authenticated Communication Scheme for Smart Grid

Sneha .U, Liji Samuel

M.Tech CSE
Sree Buddha College of Engineering Elavumthitta, Kerala 689625
Assistant Professor of CSE
Sree Buddha College of Engineering Elavumthitta, Kerala 689625

Abstract

A "smart grid" is a reading meter which includes a various application and unit measures including reading meters. Smart meter collect the daily time information. Smart meter collect daily data and that data is encrypted. The main aim of this paper is to compare the existing systems with LAC scheme an various concepts used in LAC of secure communication data exchange. This survey paper presents the different techniques which is used in LAC of secure communication data exchange.

Index Terms-Smartgrid, sensors, lightweight, authenticated Communication.

I. Introduction

By comparing different security techniques. The introduc- tion of smart grid is the secure two-way message exchange. The system is used in this technique. The connection between smart meter and system. The security provide using key exchange technique. The key exchange technique is used for avoid the third party attacks. The third party attack is used to user A can be send message to user B, but do not give message to user B. The third party is take that message after that message is changed then this changed message is send to user B. The key exchange technique is used for provided security.

Key exchange is the user A select the private key and calculate the public key. After calculated public key is send to user B. The user B of the public key using generate the secret key. Similarly user B select the private key and calculating the public key. That public key is send to user B. The user A of the public key using generate the secret key. The encryption and decryption performed using that key. Then next is used for secure two-way data transmission. The communication of the smart grid is consists of three layers. Higher layer ,lower layer and middle layer. The advantage is communication cost of reading meter can be reduced. The data transmission between reading meters and the NG can be performed in a high security manner. Compared with other old schemes, and the new scheme is both low storage and low communication cost.

II. Related Works

Reading meter is used to daily collected unit reading. It consists of three layers. Top layer middle layer and bottom layer. The bottom layer is connected to the home network. It consist of reading meter and home systems. The middle layer is connected to the nearest area networks and more home network are connected to the nearest networks. The top layer is the wide area network that is controlled by power thesaurus. The reading meter take the daily unit data that data is enciphered. This data is send to nearest networks. The nearest information receive the unit data back send to the power thesaurus with the received unit information and power thesaurus take the action and send control information to the nearest network and the correlated reading meter.

From the [2] proposed a design activity. The reading meter design activities are listed below: 1) Security: Our information is secured that means information is do not access any other peoples.2) Daily-time security for messages: The sending unit message can be real timely secured by the receiver.3) Storage space and communication: The storage and communication payment of the reading meter should be small due to the events limited resource.

[3] Proposed by security and privacy the security provided for reading meter is secure two-way message sending. The secure two-way message sending is the first select the 96 arbitrary values. Then apply digests value to it. After that we enciphered the nearest network arbitrary value. Then it also apply to digests function. Then we get 96 big values, and performing Boolean function. Then r1,r2,r96 converted to c1,c2,c98 in function each has value corresponding to its. The terms of protection. Reading meters also have unexpected outcome for people privacy. Unit use message stored at the meter. The daily collect the data to each home that data is securely transmitted to the power synonyms. That message is enciphers. Do not take this message is third party or any other persons. It provide the all security provided to daily usage unit data.

Service antonyms [4] proposed cost message, meter information, control commands, software, total unit billing sensors information and usage information (e.g., people registration and service related information) are the main information transmitted in service applications. The development of reading grids, while more types of data will be transferring. Main data is provide a sample of security problems in service applications. Power uses and then obtains a pk certificate for its identity and Pk are saved in every reading meter before installation.

Chance of security attacks in home-area-based networks, user only entity responsible for the operation of the network. For example, consider the case of a house system. It is in the interests of the user that the network functions permanently used. A typical security attacks possible on a wireless network, the reading-meter scenario has the additional dynamic of there being two peoples with interests in the network. If the reading meter exchange network does not function permanently, it prevent the users.

[5] Proposed the same enciphering operations (HE) tech- nique is the form of enciphering and generate the enciphered result. After it check whether the enciphered and deciphered message is same or not. HE is usually used for privacy- providing operations (e.g., data aggregation, e-voting).

A privacy-preservation of [6] electricity demand in the new power center scheme, since home peoples power center demand is a HE ciphering . It cannot identify the corresponding power center data even though a eavesdrops the ciphering. It only aggregates and does not deciphering the power center, it do not get the power data . Formulation of a New Attack in a reading meter .In reading grid, one differentiate reading grid. communication networks is the top-scale deployment of sensors and reading meters. Thus, a large amount of data and information will be generated from metering. The large amount of data is generated in sensors communication networks, Information from meters should be real-time delivered and processed for power center . Thus, data aggregation services in sensor exchange networks is a critical design problem.

Key methods is a security-maintaining scheme and a HE to serving security-maintaining scheme and well planned replay. In additionally, an key technique is used to ensure the peoples SK to be send secure.. In comparison with an old scheme which also achieves sending secrecy, well planned in terms of computation communication overheads and can adaptability control the exchange security mechanism. The key is used to provide the security of all information. Key is the security mechanisms.

(SG) communication scheme [7] is the secure data authenticating synonyms scheme to the power management center. However, communication trust and security problem introduce practical concerns to the unfold . In this scheme t a LAC scheme features as a basic for secure SG exchange scheme. Specifically, in the new scheme, the reading meters which are distributed at different layering networks of the security shared SK with DH exchange protocol. Then, with the SK between reading meters and hashing synonyms code technique, the information can be secured a LAC scheme.

Propose a tree reading meter [8] has emerged as the next phase of power center through its reliable, flexible. However, reading meter faces some security such as the message attack and the replay attack. If these security cannot be permanently addressed, replay information attacks to low the performance of sensors. Specifically, the new security scheme considers the reading meters with computation-constrained organiza- tion. Completed security checks represents its security power, namely, resilience to the response attack, the message attack. In extra, performance analysis and its terms of computation complexity and exchange methods. Responds attack: This attacks is the back to the messages is to delivered. That message is changed. Information attack: The information is changed from the original messages.

The secure group message transmission [9] each time SK need to be shared among cluster peoples in a secure types. In this new improved security key sending method based on secure sharing. The new method key confidentiality due to security of message to all peoples. Furthermore, the new method protect both incoming and outgoing attacks. There are people in a cluster. To perform secure transmission, the cluster SK are needed to be securely described among all peoples prior to share messages. Typically, choose new SK and securely distribute them, in a way that only peoples can generate the SK upon delivered the data. In an improved secure key transfer based on secret exchange.

A password security key method [10] proposed using reading meter. The scheme has many applications, it that it prefer from three types: 1) password-changing operation; 2) the SK problem; and 3) the twice SK. Therefore, an improved quality and performing the application of the original scheme. In addition scheme minimize the storage and computation payment on the reading card compared with the method performing scheme is more suitable for real-life applications new a password-key agreement scheme using reading cards. In this method and new performing method not only preserves the application of the scheme but also represents its disadvantages. In extra, method minimize the storage and computation payment on the reading card compared. Therefore, it that method is most suited for real-life applications.

[11] propose a (WSNs) have been widely used as a promising solution for difference operation of power center and realizing the vision of sensor. However, creates a number of challenges for WSNs, as a result of which energy and reliable become must. On the other hand, (CR) technology is accepted to open a role in sensors networks. The CR equipped sensor networks [or cognitive sensor networks (CSNs)] can effectively address the individually. In this to design a reliable (MAC) for CSNs. Moreover, high reliable can be provided the large number of destinations. In extra CRB-MAC good security is provided.

III. Conclusion

In this paper, a LAC scheme using boolean and LI formula to encipher and secure data transmitted in SG. Security analysis seen that the new method can achieve secure two-way exchange between the reading meter and the nearest gateway. A nice feature of the method is that it can significantly minimize the storage and communication payment compared with old methods. This paper discuss its advantages and disadvantages.

DOI: 10.18535/ijecs/v6i1.51

References

[1] Yining Liu, Chi Cheng, Tianlong Gu, Tao Jiang, S and Xi angming Li, "A Lightweight Authenticated Communication Scheme for Smart Grid,"IEEE SENSORS JOURNAL.VOL. 16, NO. 3, FEBRUARY 1, 2016.

[2] G. W. Arnold, "Challenges and opportunities in smart grid: A position article, " in Proc. IEEE. vol. 99, no. 6, pp. 922 - 927, Jun. 2011.

[3] F. P. McDaniel and S. McLaughlin,, "Security and privacy challenges in the smart grid," IEEE Security Privacy. vol. 7, no. 3, pp. 75 - 77, May/Jun. 2009.

[4] D. E. Nordell, "Terms of protection: The many faces of smart grid security," IEEE Power Energy Mag.vol. 10, no. 1, pp. 18 -23, Jan./Feb. 2012.

[5] C.-H. Lo and N. Ansari, "Decentralized controls and communications for autonomous distribution networks in smart grid,",IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 66 - 77, Mar. 2013 .

[6]] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Network security management and authentication of actions for smart grids operations," in Proc. IEEE Canada Elect. Power, Oct. 2007, pp. 31 - 36.

[7]] X. Li, X. Liang, R. Lu, H. Zhu, X. Lin, and X.Shen , "Securing smart grid: Cyber attacks, countermeasures, and challenges," IEEE Com- mun.Mag, vol. 50, no. 8, pp. 38 - 45, Aug. 2012.

[8] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," IEEE Syst. J,vol. 8, no. 2, pp. 598 - 607, Jun. 2014.

[9] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 375 - 381, Jun. 2011.

[10] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communica- tions," IEEE Trans. Smart Grid,vol. 2, no. 4, pp. 675 - 685, Dec. 2011.

[11]] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle tree- based authentication scheme for smart grid," inIEEE Syst. J., vol. 8, no. 2, pp. 655 - 663, Jun. 2014.