IJICTR
International Journal of Information & Communication Technology Research

Volume 11- Number 4 – Autumn 2019 (21 -28)

A Secure Protocol in Smart Metering Networks Based on the Internet of Things

Mona Shahsavan
Department of Electrical Engineering, Faculty of Engineering and Technology, West Tehran Branch, Islamic Azad University, Tehran,

Mahdi Eslami*
Assistant professor, Department of Electrical Engineering, Faculty of Engineering and Technology, West Tehran Branch, Islamic Azad University, Tehran,

Pedram Hajipour
Faculty member of Satellite Communication Group, Department of Communication Iran Telecom Research Center, Tehran, Iran.

Received: 1 May 2019 - Accepted: 16 August 2019

Abstract—**In this paper, a secure chord protocol based method is presented to improve the latency and system storage requirements in smart metering. In the proposed approach, a secure multi-mode computation method is utilized which can reduce the time of data exchange and memory consumption, by maintaining data security and subscriber's privacy. This method can be utilized in smart metering networks based on the internet of things (IoT). According to the simulated results, the proposed method incremented the amount of production capacity by 26% compared to the reference model. Also, the average time to complete the data collection reduced by 65.5%, and the package delivery ratio of the proposed model incremented by 14.4 % in comparison with the reference model. Also, a secure mechanism-based lightweight authentication was provided. This scheme needs half memory usage versus other security plans such as the EDAS algorithms**.

Keywords-component; Smart meter; Secure communication; Internet of things ;Data encryption; Bloom filter

I. INTRODUCTION

Today, the creation of communications in IoT based smart grid systems is the focus of the attention of engineers and designers in various industries. Smart grids are considered as a safe and reliable network with the aim of better managing the amount of energy demanded by subscribers and reducing environmental pollutions. It should be noted, however, that security issues must be considered at the same time as the privacy of the subscribers and the security of the measured data. Therefore, providing algorithms to create security will be a serious challenge. In these algorithms, the encrypted data need to be authenticated by the energy distribution center before any action, and the actual and malicious data must be separated from each other.

In general, the smart grid includes smart sensors and electronic devices that are deployed along transmission and distribution lines and are smart meters on the consumer side. In these types of networks, a smart meter detects and collects the amount of power consumed by consumers electronically or manually [1]. Fig.2.show the overall structure of a smart grid and the relationship between different parts in them. As illustrated above, the

* Corresponding Author

communication infrastructure of the smart grid is separated from the electrical distributed infrastructure. The smart grid includes the hardware part, software part, and the relation between them. In this type of structure, consumer information such as consumption, voltage, the current is received. This network is able to read, configure, monitor, and remotely control the metering, processing, and analysis of collected data by establishing a two-way communication path. It should be noted that all these processes will be automated [2]. In Table 1., the traditional and smart networks in terms of their elements and specifications were compared together.

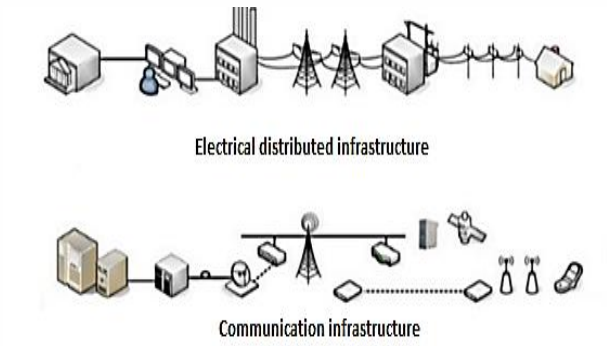

Figure 1. Smart grid network [3].

TABLE I. COMPARSION BETWEEN TRADITIONAL AND SMART GRID NETWORKS

Traditional network which include:	Smart grid network which include:
Electromechanical devices	Digital devices
Without smart sensors	Many smart sensors
One-way communication	Two-way communication
Manual operation	Automatic and remote operation
Limited control	Control with telecommunication network
Central generation system	Distributed generation system
Deactivate consumer	Active consumer

Generally, the purpose of smart meters is to establish a two-way relationship between the consumer and the manufacturer in a stable situation and reliable manner with respect to privacy [4]. Of course, to deal with some of the concerns of consumers, we can collect the existing data privately and securely from inside the network. In order to secure the collection data process, a Fully Homomorphic Encryption (FHE) method is used to make the required mathematical calculations. However, it can be used to collect data from other methods such as data encryption at the source and then send them to the destination. Two security methods based encryption in these types of networks include Partially Homomorphic Encryption (PHE) and FHE. In this case, the data first can be encrypted with approximation or complete encryption. Finally, using the Secure Multiparty Computation has been used to perform calculations on these data [1]. In this paper, we discussed these methods and computation solutions in a distributed power center. The first partially approximation method (PAM), due to the advantage of aggregation and smaller message expansion features and security has been widely proposed for collecting data in smart metering [5].

In real examples, there are many intelligent metering networks based on the above algorithms. These types of networks can execute the aggregation process at each level of the three topology levels such as the consumer side, the cloud space between the transmitter and receiver, and gateway. While other software performs the aggregation process on the output gateway. For example, the end to end collection data software has been implemented in the terminal based on the simple Paillier (Pai) cryptosystem and the advanced encryption systems [6, 7].

The FHE was proposed by using the digital signature Elliptic Curve Digital Signature Algorithm) ECDSA) in 2009 [8]. This method was a successful solution to achieve a full encryption method. Of course, compared to other networks, it produced larger-scale encryption schemes and encrypted text. In some places, this type of encryption would cause excessive noise and it causes to implement far from reality [9]. Smart-Vercauteren (SV) scheme looks like an FHE system that has encryption and decryption keys. Also, it has multiplication and decryption parts. This type of scheme provides public and private key to Encrypt information [1].

To this end, an FHE scheme with relatively small key modes and text size was proposed [10]. This type of method has advantages and disadvantages; one of the advantages is the approximate maintenance of data security. But one of the disadvantages includes not considering the size of packages in the rebuilding process. To date, little research has been done on the use of secure multitasking protocols to collect data on smart grids.

In [11,12], the application of A secure architecture and a secure protocol is used to collect the measured data in which a type of decryption is used to maintain security and privacy in collection data. Of course, another study for smart meter is proposed based on load management, and providing billing framework was provided based secure multiparty computation (SMS) with Pai decoding [13,14]. This scheme is applied to the PHE system. This type of scheme can perform not only homomorphic but also, operation on text encryption. Finally, the secure multiparty computation (SMPC) is used for data aggregation and performs arithmetic operations based privacy-preserving method [1]. In order to maintain the security of the measured data and to protect the security of the consumers, a plan should be used that is of little computational complexity. Also, prevent the distortion of measured data. It also prevents them from being compromised. Ultimately, using this method should also reduce the processing time and the process of transferring, receiving, and verifying, while

minimizing the memory it occupies to store data. According to provided references for data security in smart meters, encryption methods are used to protect data security and privacy, but sometimes computational operations are performed on data. Therefore, the encryption will take hours or not all operations on this encrypted data will be executed. So, it is important that there is a plan for secure data to transfer in the smart grid. In this paper, we are going to introduce different secure protocols from what has been done in other researches to protect data and consumer security in the smart grid. In addition to maintaining security, our security protocol will improve the key parameters including Through Put (TP), Average Data Collection Completion Time (CT), and packet delivery ratio (PDR) during the data collection process. The encrypted data transfer requires an authentication plan after transmission. In some cases, the authentication plan causes a lot of time, memory, and overhead in the system. To improve this problem, we will consider a lightweight authentication scheme. Then we will provide a transmission data plan without authentication. In this scheme, the data are validated with a filter and compared with initial data. The purpose of this scheme is to improve the time, memory and communication overhead for the encrypted data without the complexities of encryption. In the process of this lightweight authentication, public and private keys are created during the data exchange process. Also, secure data exchange is done when two interconnectors confirm each other. The procedure for implementing this approach can be as follows:

1. In the first step, all measured data are inserted in the destination bloom filter with the hash process and finger table.

2. In the second stage, the measured data transmitted by ring protocol from consumers to the center (like a power distribution center)

3. In the third stage, after the data are removed from the loop structure, we return them to a center bloom filter. Then, we compare the output results of the center bloom filter with the destination filter. The output of this filter is expected to be identical to the destination bloom filter. In this case, the data have been accomplished without any changes and with complete integrity and accuracy. Otherwise, the source of the request has to be returned from the source.

In Fig.2, the proposed structure block is presented. In the next section, some of the tasks that have been done on the safe transfer of data are summarized. In the third section, we provide the details of the proposed secure protocol, and in the fourth section, we evaluate the efficiency of the proposed design in terms of the three main parameters of production capacity, average time collection, and packet delivery ratio. Also, we provide a security mechanism based lightweight authentication.

II. DETAILS OF THE PROPOSED SYSTEM MODEL USING OF BLOOM FILTER AND RING PROTOCOL

This section of the article first provides an explanation of how the filter works in the proposed scheme. The second part describes how the loop protocol works to transfer data from the consumer to the center. Finally, in Part III, the application of this type of secure protocol in the proposed system model will be explained.

III. STRUCTURE OF THE BLOOM FILTER IN THE PROPOSED SYSTEM MODEL

In 1970, a person with the name of Burton Howard Bloom introduced, for the first time a random data structure. This structure was named a bloom filter later [15]. The bloom filter is an m- bit array with n elements and k time of hash operation. It is assumed that all its locations are zero. In order to insert the elements, the hash operation must be first performed. The amount of locations will be changed to one. The accuracy of a Bloom filter depends on the size of the filter and the order of hash used in the filter and the number of set elements. These filters have four important modes: false negative, false positive, false-positive, and false-negative. Whenever a large number of elements are inserted into the Bloom filter, the likelihood of a false-positive response is increased, meaning that an element in the bloom filter is declared not a member of the dataset. In this situation accrued when an element in the bloom filter that is not a member of data collection. Equation (1) shows the probability of a false positive response of a set [16].

$$F = \left[1-\left(1-\frac{m}{n}\right)^{n\times k}\right]^{k} \approx \left(1-e^{\frac{k\times n}{m}}\right)^{k}. \qquad (1)$$

In the above equation:
m: length of a bloom filter according to the number of available bits.
n, the number of smart meters available.
k: number of times of hash in the bloom filter.

IV. STUDYING THE STRUCTURE OF RING PROTOCOL IN THE PROPOSED MODEL SYSTEM

The ring protocol was introduced by Gentry and several others. In fact, it consists of a network consisting of nodes, keys, and Consistent hashing [17]. Three features that distinguish the ring protocol from many other protocols are simplicity, proven accuracy, and acceptable performance. In fact, there are a number of keys and nodes in the network structure that the hash function is applied with m-bit identification which applies on each node and the key continuously.

The ring protocol was introduced by Gentry and several others. In fact, it consists of a network consisting of nodes, keys, and Consistent hashing [17]. Fig. 3 shows a simple example of the secure protocol with the ten existing nodes (N) and the five available keys (K). In order to retrieve and call for this protocol in the destination, a finger table [17] is used to call exciting data.

Each node has an identifier and a key that after reassembling will be generated a new name for each of them. We will use the same name for the primary and secondary keys and nodes to simplify the expression. As seen in this figure, the successor of the 10th identifier is the 14th node, which is the first value of which the10th identifier is smaller than it and it is a clockwise direction. Therefore, the 10th key will be placed at the 14th node. In addition, the first node whose identity value is smaller than K and it is clockwise direction is for 24th and 30th identifiers in the 32th node. Therefore, the 32th node is assigned to 24th and 30th keys and so the whole loop will be formed.

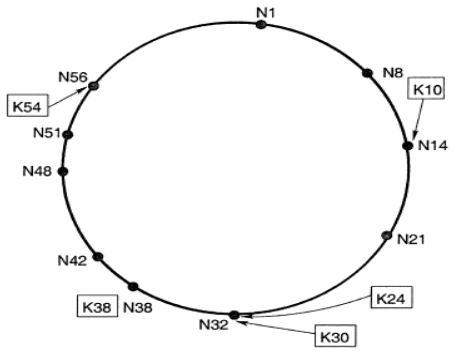

Figure 2. Ring Protocol with 10 nodes and 5 keys [17].

V. EVALUATION OF THE PROPOSED SYSTEM MODEL

In [1], a protocol is used to create encryption of the existing information in a smart grid. Also, this type of information extracted by a multi-state calculation. In this structure, the encrypted information is collected in several smart meters and will be directed to the destination of the distribution network. The results of the review in [1], shows that this type of structure can be a reliable way of gathering information with privacy, as long as it does not diminish the security of data and consumers. Of course, if this structure is used in an advanced smart metering network of larger dimensions, this structure will not work well.

Therefore, in our proposed system model, all measured values by the meters have a hash process with a finger table in bloom instead of an encryption process to transmit. If we assume that the order of the hash function for each of the meters in the proposed model system is 3 based on Ref.[18], the measured data can occupy three locations of the bloom filter, and their values can be changed from zero to one with respect to the data of the bloom filter. In the next step, the measured data are presented to the ring protocol. The original value of the measured data is contained within the nodes in the loop protocol. Finally, the data sent hierarchically to the power distribution center. At the power distribution center, these data stored in a center bloom filter, and the results are compared with the primary filter. The purpose of this is to verify the accuracy of the packages that will eventually be delivered to the power distribution center. If the output of this filter is the same as that of the destination bloom filter, then the data can be safely and delivered to the center without any changes. Otherwise, we will stop the process and declare the collected data are invalid and the transition process from source to the center must be repeated. In Fig. 4, an example of the mismatch of the center bloom filter with the destination bloom filter om the receiver side.

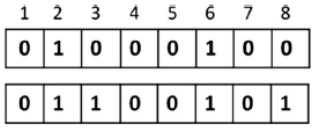

Figure 3. Comparison between the destination bloom filter and the center bloom filter [15].

The advantage of this method versus previous methods is that throughout the process of transferring the hashed identifiers represent the measured data and the data security is fully maintained. In the above scheme, data recovery is performed on the basis of a reference table. Therefore, the search speed and time complexity would be acceptable. Also, the intermediate meters receive the data of the previous meters in a concatenated way. Therefore, they cannot detect and maintain the confidentiality of the measured values. Finally, the non-distortion of the data content is measured by inserting it into the bloom filter. If the data are not verified, the data are discarded and the re-measured values are taken from the meters. Totally, to measure the performance of the proposed design, three main parameters including production capacity, meantime completion time, and packet delivery ratio, and its value are compared with reference results [1]. The simulation is also performed by increasing the number of meters to achieve a real sample. In this simulation, the total amount of data received by each gateway per second is expressed as output capacity. Due to the processes used in the proposed scheme, it is expected to search and reconstruct data centrally based on the layout of the annotation in the loop structure that is expected to produce the proposed scheme for sending and receiving data has been improved. In Fig.5, a comparison capacity between Ref.(1) and the proposed system model, as can be seen in the proposed scheme, which can increase approximately 26 percentage with increasing the number of smart meters.

TABLE II. PARAMETERS CONSIDERED IN THE PROPOSED MODEL SYSTEM

Parameters	Values
Number of iteration	5
Length of simulation	100 (s)
Number of meters (n)	[30,40,50,60 and 70]
Duration of the bloom filter (m)	100 (byte)
Number of the hash operation in bloom filter (k)	3

VI. SIMULATION OF THE PROPOSED SYSTEM MODEL

In order to simulate the proposed model system, MATLAB software was used. The proposed simulation

is done using a maximum of 70 smart meters for 100 seconds. In this system, model is assumed that the value of the meter size is between 1 and 200. Also, the length of the bloom filter is considered to be 100 and the number of hash for the measured value for speed and ease of computation is three. The simulation parameters are given in Table 2.

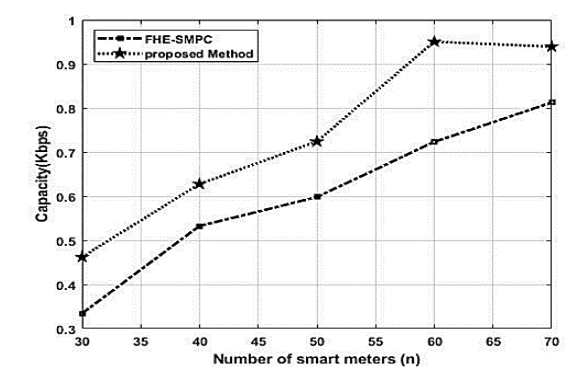

Figure 4. Comparison between production capacity of proposed system model and Ref. [1]

Generally, the average time taken to obtain all readings from all smart meters in a data collection center in a period is called the time to complete the data collection. Instead of using sophisticated cryptography and computation, we use loop and hash structure to expect to reduce the total time wasted for computation as well as data collection completion. In Fig.6, the amount of time spent to obtain all reference values [1] and the proposed system model, as observed, the amount of this time in the proposed scheme can be approximately less than 65.5 percent higher than the Ref.(1).

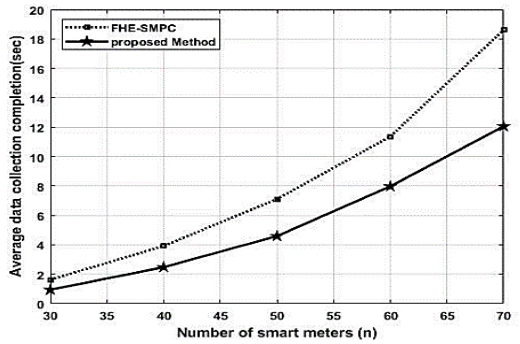

Figure 5. Comparison between average data collection completion of proposed system model and Ref. [1]

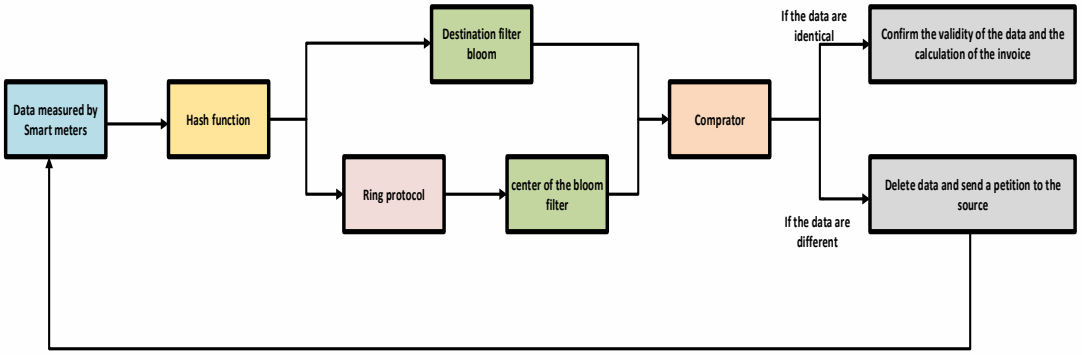

Figure 6. System model based on the secure protocol.

Also, the proportion of packets delivered to the data collection control center is reported as the proportion of packets sent by smart meters. If the data collection process is based on blending and insertion into the bloom filter to validate the data, the distortion of the data is detected at the intermediate nodes and the valid data will then be re-requested. On the other hand, by merging the identities and inserting them into the loop structure, we will be able to maintain data confidentiality so that data can be properly received at the control center. As a result, the number of packets that are properly controlled is increased. In Fig.7, the comparison between the packet delivery ratio in reference [1] and the proposed scheme, as observed, is approximately 14.4 percent higher than the Ref.(1) in the proposed system model. A comparison between simulation results of the proposed system model was shown in Table 3. Due to the qualitative and quantitative comparison of the three types of schemes, the Paillier cryptosystem is applied to simple aggregation. Therefore, it cannot be used for additional functions such as encrypted data.

SV and secure MPC schemes apply for both addition and multiplication on the encrypted data. These types of schemes can use different operations with respect to privacy of the consumers.

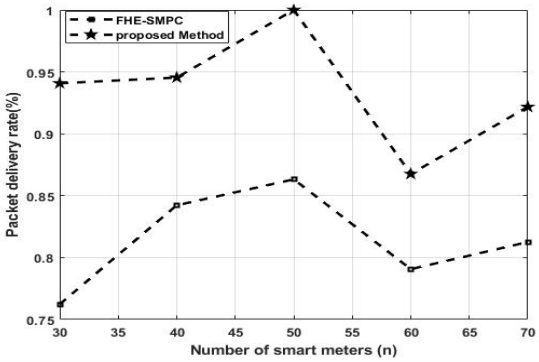

Figure 7. Comparison between packet delivery of proposed system model and Ref. [1]

TABLE III. A QUALITATIVE AND QUANTITATIVE COMPARISON OTHER RESEARCHES IN IN SIMUATION RESULTS

Number of smart meters (n)			30	40	50	60	70
PDR (%)	Provided system model	Ref. [1]	0.76	0.83	0.85	0.87	0.81
	SV		1	1	1	1	0.98
	Pai		1	1	1	1	0.97
	SMPC		1	1	1	1	1
	Proposed system model		0.94	0.95	1	0.8	0.93
TP (Kbps)	Provided system model	Ref. [1]	0.48	0.6	0.7	0.95	0.95
	SV		2.1	2.9	3.9	4.7	5.1
	Pai		1.6	1.8	2.1	3	3.2
	SMPC		0.3	0.4	0.5	0.6	0.7
	Proposed system model		0.2	0.5	0.6	0.7	0.8
CT (S)	Provided system model	Ref. [1]	2	3	6	10	15
	SV		16	21	34	40	49
	Pai		8	12	17	19	21
	SMPC		12	16	19	21	29
	Proposed system model		3	7	12	20	27

VII. PROVIDING SECURITY MECHANISM BASED LIGHTWEIGHT AUTHENTICATION

In the lightweight authentication solution, the data is encrypted with the public key of the building meter. If the public key encryption method was secure and approved, the building meter retrieves the data with the corresponding private key[19].

When the home meter receives the correct data with the key generated in the process, it can be assured that the meter connecting is the corresponding building meter. Therefore, the communication and data exchange is secure with it. Similarly, each data encrypted with the public key of the home meter, if the building meter can receive the correct data, it will authenticate and confirm the home meter and finally, the connection between the two building meters will be secure. The proposed scheme can provide a cross-authentication method between the home and the building meters.

Therefore, a lightweight authentication solution can provide a secure shared key. If the security of the home or building meter is in unsuitable action, the cross-verification process will not be compromised. Therefore, the connection between the home and the building keys does not affect the security of the other keys. As a result, this lightweight authentication scheme can be a good solution for confidentiality.

Lightweight authentication can provide encryption and channel authentication for the successful transfer of delayed data. Because both of the home and the building meters maintain the shared key section. Besides, the delayed transitions not only remain confidential but also maintain their integrity and accuracy. Because they have a specified time tag. Therefore, a lightweight authentication and encryption process can be provided for delayed transmissions. This lightweight authentication scheme is compared to the EDAS plan. This plan has a key length equal to 256. For comparison, lightweight authentication and the EDAS have been simulated.In this simulation, only the messages exchanged between the home network and the building network are intended for authentication. In addition to constructing, the key of each segment was done at the start of each new round of data collection.

In this section, the lightweight authentication scheme over time is discussed below. The simulation results are presented on a limited and overall scale in Figures 7 and 8, respectively. These simulations are performed from 0 to 80 seconds. These two outputs are simulated by considering the number of meters is constant over time.

As we have shown, the volume of messages received per home communication network in the proposed scheme is lower than the EDAS structure. Despite of the fluctuations in the values obtained, the results show a good improvement of the performance of the proposed scheme over the time. Therefore, in the most of the simulation times the proposed structure,

need lower memory usage versus EDAS plan. In Figures 7 and 8, the comparison between the proposed scheme and EDAS, as observed, is approximately half of the proposed system model.

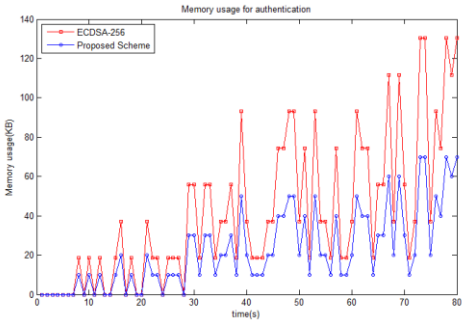

Figure 8. Memory lightweight authentication scheme over time in 2 seconds with small scale counters constant.

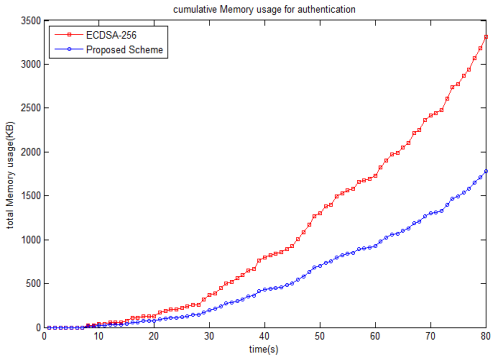

Figure 9. Memory lightweight authentication scheme over 5 seconds with large scale counters constant.

In the next step, the amount of memory usage is evaluated based on the variable number of meters, and the outputs are shown in Figures 9 and 10.

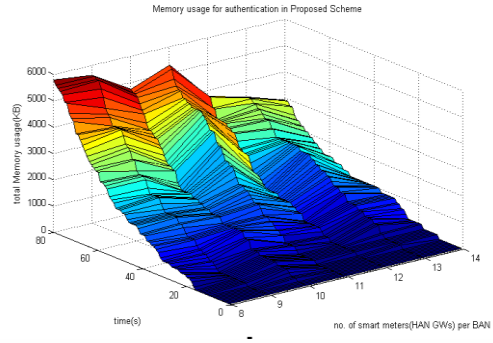

Figure 10. Memory lightweight authentication scheme over time in 6 seconds with variable number of meters.

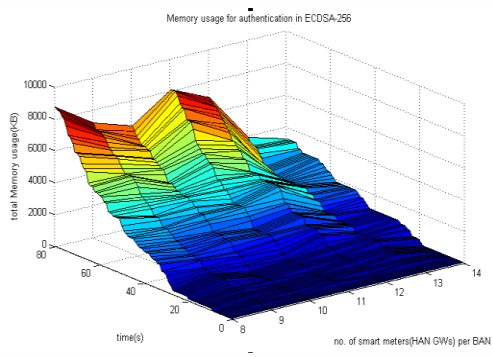

Figure 11. Memory consumption of elliptic curve authentication scheme over time in 5 seconds with variable number of meters.

As shown in Figures 9 and 10, the amount of memory usage in the lightweight authentication scheme is substantially less than the EDAS scheme. This will improve system performance when large amounts of data are sent concurrently to the building meter. Besides, we show the impact of the number of meters on the average communication overhead. As it is observed in Figures 11 and 12 by increasing the number of smart meters, the average communication overhead versus EDAS-256 increases for small and large scale in 80 seconds.

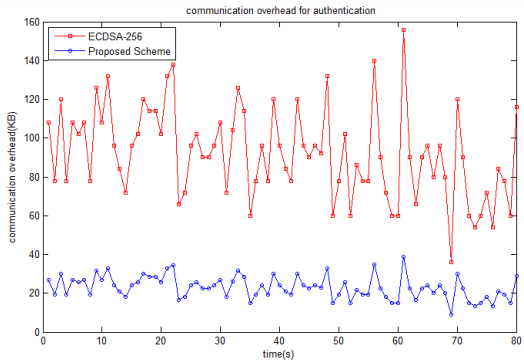

Figure 12. Lightweight authentication scheme communication overhead with fixed meter count in 80 seconds on a small scale.

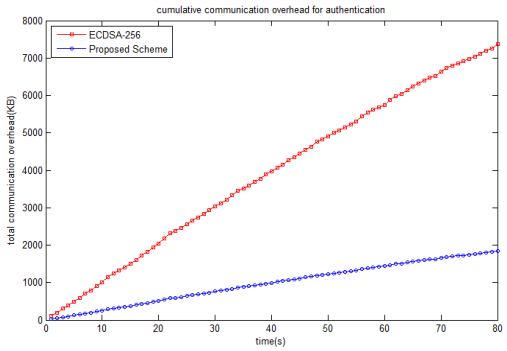

Figure 13. Lightweight authentication scheme communication overhead with fixed meter count in 80 seconds on large scale.

It should be noted that the communication overhead of the lightweight authentication scheme by increasing the number of smart meters from 1 to 14, will remain constant from n=5 and after that.

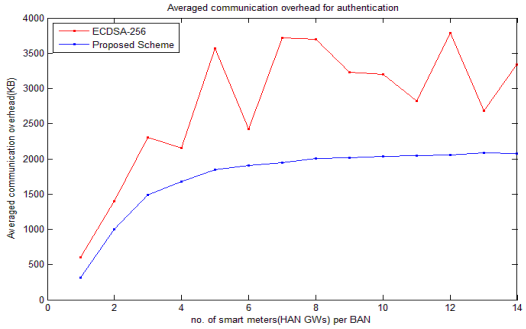

Figure 14. Lightweight authentication scheme communication overhead with incrasing smart meters from 1 to 14.

VIII. CONCLUSIONS

In this paper, a security protocol for IoT based smart networks is introduced. In the structure of the above protocol, instead of using complete and approximate

homomorphic encryption methods, the method of scrambling is used by a finger table.
In this case, the numbers are stored in the Bloom filter according to the position specified in the finger table and compared with the results of the other Bloom filter in a parallel path. If the output results of the two filters are identical, the bill is extracted. Otherwise, the receiver will request the transmitter to send bill information, again. This process has enabled data transfer while maintaining complete security and improving system output parameters such as capacity and latency.

REFERENCES

[1] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems", Future Generation Computer Systems, vol. 78, pp. 547-557, 2018.

[2] Available at:http://www.pooyeshqeshm.com/proser/ami.html.

[3] Available at: https://5g.itrc.ac.ir/sites/default/files//5G-for-smartrid-961202.pdf.

[4] Hassan, M. U., Rehmani, M. H., Kotagiri, R., Zhang, J., & Chen, J. ,"Differential privacy for renewable energy resources based smart metering", Journal of Parallel and Distributed Computing, vol.131, pp.69-80, 2019.

[5] U. Ozgur, S. Tonyali, K. Akkaya, and F. Senel, "Comparative evaluation of smart grid ami networks: Performance under privacy", Proceeding of IEEE Symposium on Computers and Communication (ISCC), pp. 1134-1136, 2016.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", Proceeding of International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 223-238, 1999.

[7] U. Ozgur, S. Tonyali, and K. Akkaya, "Testbed and simulation-based evaluation of privacy-preserving algorithms for smart grid AMI networks", Proceeding of IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops), pp. 181-186, 2016.

[8] Fournaris, A. P., Dimopoulos, C., Moschos, A., & Koufopavlou, O, "Design and leakage assessment of side channel attack resistant binary edwards Elliptic Curve digital signature algorithm architectures", Microprocessors and Microsystems,vol. 64, pp.73-87, 2019.

[9] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and cipher text sizes", International Workshop on Public Key Cryptography, Springer, pp. 420-443, 2010.

[10] Rahman, M. S., Khalil, I., Alabdulatif, A., & Yi, X. ,"Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform. Knowledge-Based Systems", vol.180, pp.104-115, 2019.

[11] C. Rottondi, G. Verticale, and C. Krauß, "Secure distributed data aggregation in the automatic metering infrastructure of smart grids", Proceeding of International Conference on Communications (ICC), pp. 4466-4471, 2013.

[12] C. Rottondi, M. Savi, D. Polenghi, G. Verticale, and C. Krauß, "Implementation of a protocol for secure distributed aggregation of smart metering data", International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), pp. 1-4, 2012.

[13] C. Thoma, T. Cui, and F. Franchetti, "Privacy preserving smart metering system based retail level electricity market", Proceeding of IEEE Power & Energy Society General Meeting, pp. 1-5 ,2013.

[14] C. Thoma, T. Cui, and F. Franchetti, "Secure multiparty computation based privacy preserving smart metering system", North American power symposium (NAPS), pp. 1-6, 2012 .

[15] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422-426, 1970.

[16] S. M. S. Amiri, H. T. Malazi, and M. Ahmadi, "Memory efficient routing using bloom filters in large scale sensor networks" ,Wireless Personal Communications, vol. 86, no. 3, pp. 1221-1240, 2016.

[17] I. Stoica, R. Morris, D .Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," ACM SIGCOMM Computer Communication Review, vol. 31, no. 4, pp. 149-160, 2001.

[18] P. Goudarzi, H. Tabatabaee Malazi and M.Ahmadi," Khorramshahr: A scalable peer to peer architecture for port warehouse management system", Journal of Network and Computer Applications,vol.76,pp.49-59,2016.

[19] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, 2011.

Mona Shahsavan received the B.Sc. in Electrical Engineering from Shariaty Technical College in 2014 and M.Sc. in Electrical Engineering from Azad Islamic University, West Tehran Branch of, Tehran, Iran, in 2020, respectively. Her research interests include wireless Communications and Networking, Internet of Things (IoT), Signal Processing for Fifth Generation (5G).

Mahdi Eslami received his B.Sc.degree in Control System Engineering from Tehran University, Tehran, Iran, in 1998, the M.Sc. in Telecommunication Engineering from Khaje Nasir University of Technology, Iran, in 2000, and Ph.D. degree in Telecommunication Engineering from Amir Kabir University of Technology, in 2007. Since June 2015,he has been with the Electrical Engineering Depart-ment, Azad Islamic University West Tehran Branch of, Tehran, Iran, where he is currently assistant professor. His current research interests include 5G wireless communications, digital electronics and, Internet of Things (IOT).

Pedram Hajipour received his B.Sc. in Communication System Engineering from Yadegar-e-Imam Khomeini (RAH) Shahr-erey Branch, Islamic Azad University in 2005 and M.Sc. in Communication System Engineering from K.N. Toosi University of technology in 2007, respectively. Also, Ph.D. degree in Telecommunication Engineering from Department of Communication, College of Electrical Engineering, Yadegar-e-Imam Khomeini (RAH) Shahr-e-rey Branch, Islamic Azad University in 2019. His research interests include Wireless, Satellite, Mobile and Broadband Communications and Networking, Cognitive Radio, Internet of Things (IoT), Signal processing for Fifth Generation (5G) and Self Organizing Network (SON).