Autonomous Authentication and Light Weight Key Management Scheme for Communication in Smart Metering Infrastructure

Dr.KP. Noufal[a]
[a] Assistant professor,NAM College kallikkandy, Kerala.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: A smart grid (SG) comprises several subsystems and networks which works collectively; many subsystems are vulnerable and thus are possible for attacks from remote areas. Smart Grids have evolved as the power system for the next generation which transform the standard functions of the electrical grids. In smart grids, Advanced Metering Infrastructure (AMI) is considered as one key element containing systems and networks whose major function is to collect and analyze the data obtained from smart meters. Moreover, AMI manages various power related applications and services provided are based on the data gathered from smart meters. Hence the major role of AMI is to provide smooth functions by smart grids. Malicious challengers have massive chances to attack AMI and moreover system are extremely vulnerable to these attacks. Thus, AMI has to be necessarily secured as attackers may potentially damage the infrastructure by chance and cause privacy threats in SG. Among several challenges, the two most aspects considered are producing low-latency and offering real-time services in traditional smart grid systems. Moreover, the most identified challenge is the Key Management Scheme (KMS) which plays a major role in sustaining the AMI security. To overcome these problems, block chain based authentication and four novel key management schemes are proposed in this paper for AMI aiming to produce low latency and secure data in SG. In these schemes, individual and batch rekeying function are performed with the help of a innovative multi-group key graph structure, supporting unicast, broadcast and multicast communications. From analysis, it is observed that the proposed authentication and key management schemes are efficient in preventing different kind of attacks and also reduces the management overhead. Performance analysis and security assurance are discussed which demonstrates these desirable characteristics of the proposed method.

Keywords: Advanced metering Infrastructure, Key management system, block chain authentication, unicast, broadcast, and multicast.

1. Introduction

The idea of Smart Grid has brought profitable changes in computing, controlling, automation, and communications characteristics. Concurrently, there is an emerging need to address the challenges related to security and privacy [1]. Cyber security extents integrity, computing confidentiality, availability, communications, and/or controlling devices from damage caused either intentionally or accidentally. The consequences of cyber security in SG generally disappoints because of complexity, numerous participants and devices, and operationa lconstraints which are highly sensitive to time [2]. The geographical unusual data centers collected together is termed as Computing grids [3]. When a variety of heterogeneous hardware are employed, these services jointly work with coordination to attain a common goal. Huge volume of scientific data are stored in grids and several users execute different tasks for analyzing these data in an extremely parallel and distributed way[4].

While designing a Smart Grid, the main challenge which has to be kept in mind is the level of security to be provided. This task has attracted most of the researchers [5]. SG contains various subsystems which are vulnerable to different attacks causing different harms to the resources and also in the large level to the society [6]. As SG has moved the power grid from a closed control system to the open IP networks [7] and various threats in SG are identified; few among them are man-in-the-middle (MITM), impersonation, and denial of service (DoS), which causes severe impacts towards data integrity and authenticating users as well as devices. Further, brute-force and dictionary attacks collapse data security and privacy. After entry, a malicious node or an intruder performs various tasks thereby compromising the entire system. As numerous homes are linked with SG, these attacks have impacts and causes loss or harm to the society, like power failure, changing the billing information sent to the customers and so on [8]. For secured communications, normally cryptographic keys are employed for encryption/decryption data messages. For key establishment, different methods are available for authentication.

The Smart Grid (SG), also referred as intelligent grid, intelligrid or future grid, improved electric grid which integrates information, developed two-way communication and computing intelligence to generate, distribute and manage electricity that helps in improving control, agility, efficiency, reliability, economy, security and privacy [9]. Few benefits provided by SG are greater availability of electricity at low cost for home, incorporating renewable power generation into the grid like solar or wind power, improving the security of grid, realization of successive sub-systems and producing intelligent and sustainable grid. Some of the components of grid are Advanced Metering Infrastructure (AMI), Advanced Transmission Operations (ATO), Advanced Distribution Operations (ADO) and Advanced Asset Management (AAM). AMI has been considered as the most essential component among the above-mentioned components [10]. These components play an important role in

recording the information of the customer and then transmitting then to AMI host system for the purpose on billing and monitoring [11]. Moreover, they are responsible to implement control commands like disconnecting and reconnecting remotely, controlling the devices and appliances of the customers, managing loads and demands and price signals.

In AMI systems, Demand Response (DR) program is considered as the important feature which makes smart grid more reliable and provide more benefits for the customers. DR programs are tariffs or utilities turning off the appliances of the customer. A customer has an opportunity to subscribe to various DR programs namely Real Time Pricing (RTP) program, Time of Use (TOU) program, Critical-Peak Pricing (CPP) program, and so on. For this role of AMI, it is the target for attackers causing great damage to the infrastructure and privacy of the user. On the other hand, security is the most challenging issues to be considered while developing AMI. Several requirements related to security in AMI are identical to traditional IT networks. Few requirements for AMI security are: availability, integrity, confidentiality, and accountability [12]. In order to achieve these requirements and provide secured communications, cryptographic concepts have to be implemented. However, for using cryptographic mechanisms, an efficient key management (generating, distributing, and updating) mechanism has to be developed.

When key management schemes (KMS) are poor, keys are easily disclosed to attackers, and jeopardizing is also possible which endangers the goal of secured communications in AMI. Furthermore, with numerous constrained devices, it is important that KMS must be scalable. Moreover, for the given various message transmission modes like unicast, broadcast and multicast used in AMI, versatility is a must as it has the ability to support all the above message transmission modes. Several KMS are available but none entirely support all the message transmission modes with scalability and efficiently.

Smart grid system is a kind of Industrial Internet of Things (IIoT) which possibly improves its reliability, quality of delivering energy, and feasibility. Though, for larger scale systems i.e, when customers are more in number, challenges are faced like decrease in latency and diminished QoS which has to be improved. However, attempts are made to over come these challenges, and real-time decision-making system are developed enhancing QoS and providing eco-friendly in applications that are susceptible tolatency [13], [14]. To come with security solutions for smart grid method is practically serious, since smart grids have emerged more and more in technically developed nations like US. Authentication is a measure which effectively provides trusted identity and secured communications where the communicators are identified before interacting and distributing susceptible data through the air medium [15]. Traditional protocols based on public key infrastructure are obviously unsuitable for smart grid methodology, as devices are constrained in nature. Group signature methods provide traceability and dynamic participation for smart meters but the cost for computing and communicating are high.

The upcoming part of this paper discusses about the works related for authentication and key management scheme for smart meters, proposed protocol architecture and results and discussion for the comparison of various architecture.

2. Related Works

In this section, literature related to the authentication and key management scheme for smart meter infrastructure are presented.

Kertcher Z et.al., [16] adapted Grid computing via cross-boundary collaborations. The functions of different actors and elements were integrated and produced a model of co-linking for cross-field adaptation and diffusion. Silvasi et.Al., [17]formulated bounded grids by utilizing Lean proof assistant and implemented this formalized bounded grid with an interface of several proven definitions and properties put together to manipulate grids in an usual way irrespective of the intended use case. Alrashed, S.[18] evaluated Key performance indicators (KPI) for Smart Campus and Microgrid. As there was a demand for a novel KPIs for supporting the main business of the university campus, a novel approach was developed. Every developed smart applications are not suitable for all purposes in the campus and hence suggested for assigning weights for KPIs. Badra, M.et.al., [19],introduced a KMS for smart grid applications and highlighted the practical consequences, benefits along with shortcomings. Zhang, K.,et.al., [20]developed a privacy-preserving aggregation (PARK) approach based on adaptive key management and revocation, which prevented the disclosure of user data to the untrusted parties in smart grid and implemented an adaptive KMS with effective revocation, which helped the users to update the encryption keys automatically.Das, S.et.al., [21] developed a smart grid key management framework for AMI networks. This model was analyzedwith standard protocols in a resource-constrained environment.

Tawde, R., et.al [22]integrated key distribution of CDAC and Sec-KeyD management protocol into IEC 62351 to secure IEC 61850 protocol for providing a solution for security challenges thereby eliminating the issues of key management. Latency analysis and key updating features were not discussed. Liu N.et.al., [23] coined a novel KMS to handle security issues by taking distinctive features into account. The security level was measured to estimate the efficiency of KMS. It was observed that distribution of time cost has no impact on key refreshing and traffic distribution in the network for AMI systems .Xia, J., et.al [24] propose WAMS key management (WAKE), a comprehensive key management scheme targeting a concrete set of security objectives. It was proved to be an efficient protocol for smart grid network. Law, Y. W.,[25] two multicast authentication approaches namely TV-HORS and tunable signing and verification (TSV)of power grid communications. TSV was presented with an

improved patched version called TSV+. TV-HORS and TSV+ were systematically compared and proved that TV-HORS was more efficient [26].

3. Proposed Methodologies

3.1 Authentication Method For Ami

Blockchain, a flexible decentralized database, is a novel function for storage of data distributed consensus and encryption methodology with few other techniques. This blockchain supports transactions (an important component of blockchain systems) as well as smart contracts (permanently recorded program used Turing completed language) Every contract is considered as a slot for database having unique address and transaction can be made for triggering its functions to manage the database.

The smart grid model for a network developed in this paper comprises of Authority of Registration (REG AUTH), blockchain (BLCK),edge servers (EDSRs) and end users (EDURs) as shown in figure 1.

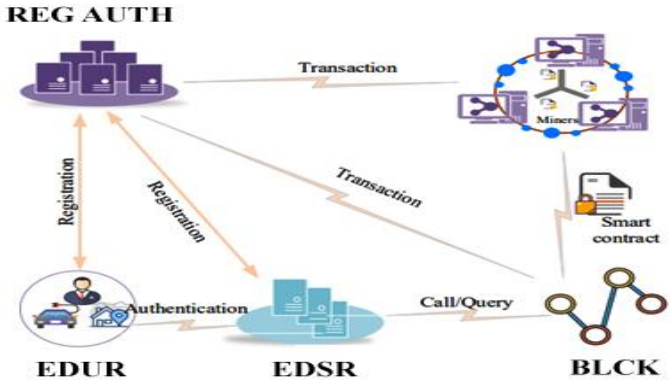

Figure 1:Network model for the block chain authentication

Authority for Registration (REG AUTH): Every participant of SG trusts this electricity service provider. The role of REG AUTH is to distribute keys to every participant and utilizes the blockchain to for recording the key materials of the participant utilizing smart contract for validating identity, updating the keys and revocation.

Blockchain (BLCK): Role of BLCK is to record the smart contract's public key materials. As this act simply like a trusted recorder to issue, update and overturning keys, most of the robust block chain systems are involved in smart grid model.

Edge Server(EDSR): This acts as an utility controller or aggregator which is having necessary computational and storing resources. Its role is for providing analysis of data and offer services on time. Every EDUR join BLCK for preventing web spoofing and ensure the normal function of BLCK. This also provides communication between few remote clouds for further data analysis or for longer storage duration.

End Users: EDURs are generally smart devices like smart meters in smart homes reporting power consumed and other relevant data to EDSR. Every EDUR can possible be connected with several EDSR but in generally only the nearest one is chosen.

In this work, the network assumptions are listed below:

The reliable records of smart contract can be accessed at any time since an attacker has only less chances to tamper the record issuing on BLCK where BLCK is essential runs a distributed ledger at all times.

Identities as well as public keys of EDSRs are familiar to EDURs. Here, the role of EDSRs generally is to act as relay nodes to provide services ontime; thereby not need to provide identity anonymities for EDSRs.

In EDSRs, key materials are frequently not necessary to be either updated or revoked, until suspected to be corrupted. When corrupted, REGAUTH revokes the server and service requests are declined from any certain or affected EDURs and present connections are shut down.

For the infrastructure of smart grid edge computing, authentication protocol must practically satisfy few important security requirements as listed below.

The REGAUTH executes the setup phase of the system initially while the system is deployed whose steps are discussed below:

1) Primary Initialization: A cyclic additive group G is selected by the REGAUTH having generator PG and prime order Q on an elliptic curve $E(F_f)$ over the finite field F_f, and two secure one way hash functions hf1: $\{0, 1\}^* \rightarrow ZQ$, $hf_2 : \{0, 1\}^{2n} \rightarrow \{0, 1\}$ 2n , where $n = \log_2 q$ is the security parameter. Then, a random number $t \leftarrow Z_Q^*$is selected by RA as the master private key and determines the relative master public key $P_{public} = t \cdot PG$.

2) Initialization of Blockchain: A genesis file is created by REGAUTH which includes configuration parameters to construct a blockchain. Then, trusted partners are selected by REGAUTH and blockchain is started following certain consensus methods. For simplicity, REGAUTH directly combines with the existing blockchain system. Secrecy is maintained by REGAUTH and public system parameters *par* = (G, PG, Q , hf_1, hf_2, P_{public}) are then published.

The proposed protocol employs the smart contract for managing the table for keys .

Pseudocode 1 : Initializing the table of keys

```
contract Keys Table
 {
 address own;
% Keys table component's structure are defined
struct KY
{
 byte32 PD;
uint256[2] X;
uint256[4] Cr;
 datatime expirytime;
}
KY[] public keys table;
% Deploying smart contract automatically constructor keys table ()
{
own = msg.send;
ln = 0;
 return 1;
}
```

Pseudo code 2 Update Keys Table

```
function update keys table (lastPD, PD, X, Cr, expiryTime)
 {
 % Update keys table.
 if own 6= msg.send then
return 0;
else
 {
if Exist(KY[i].PD == lastPD) then
{
 KY[i].PD = PD;
 KY[i].X = X;
 KY[i].Cr = Cr;
 KY[i].eytime = eytime;
return 1;
}
 Else
{
 ln++;
 KY[ln].PD = PD;
 Keys table[i].X = X;
 KY[ln].Cr = Cr;
 KY[ln].expirytime = expirytime;
 return 1;
 } }
```

Pseudo code 3. Query Keys Table

```
function query Keys Table (PD)
 {
 % specific public keys are retrieved invoked by EDSR.
if Exist(KY[i].PD == PD) then return KY;
else;
return 0;
}
```

Pseudo code 4. Revoking the Keys Table

```
 function revoke Keys Table (PD)
{
 if own 6= msg.send then return 0;
else
 {
 if Exist(KY[i].PD == PD)
{
 release(KY[i]);
for ;
```

```
 i < ln;
 i++ KY[i] = KY[i+1];
ln−−;
return 1;
}
 else return 0; } }
```

This proposed protocol will offer enhanced resilience against the attacks and supports the necessary properties of security.

3.2. LIGHT WEIGHT KEY MANAGEMENT IN AMI:

This proposed model comprises of two stages namely registration and key agreement phase.

During registration, exchange of information takes place between sub-station and Data center via secured channel. During key agreement, session key is generated by sub-station and Data center and then the authentication of these two entities is reviewed. An overall structure of the proposed light weight key management protocol is illustrated in Figure 2.

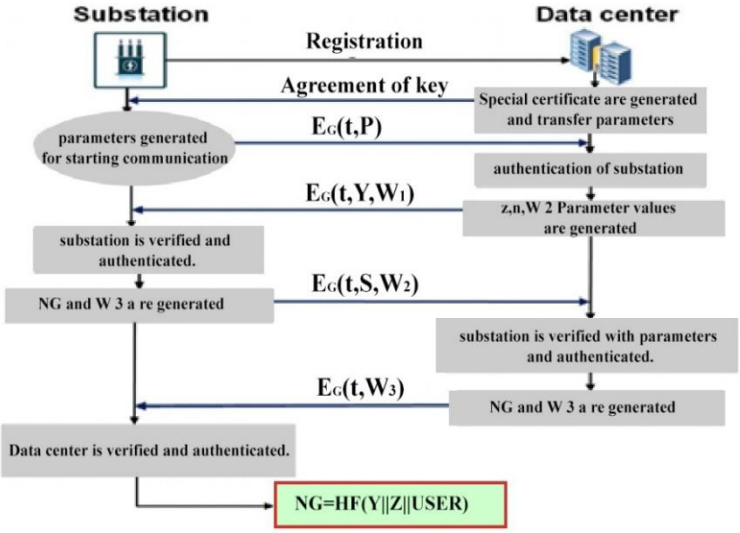

Figure 2: Proposed light weight key management protocol

Registration phase: Here, substation transmits the I and P to the Data center via secured channels. Data center produces a special certificate, after receiving the parameters, for the substation. Based on the elliptical curve, there exists various generation/authentication procedures involved in generating certificates. Authentication of substation is performed with this certificate. At last, Data center uses the symmetric key for encrypting message sent via substation and the certificate produced by the data center for substation. This phase is illustrated in Figure 3.

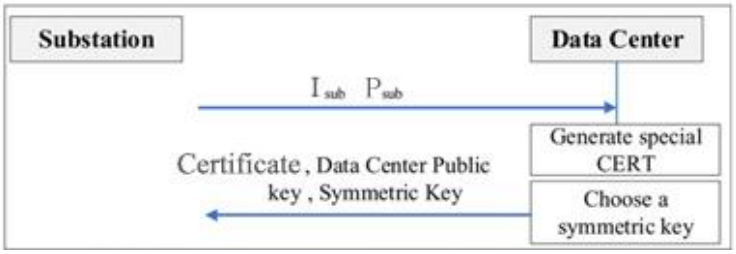

Figure 3: Registration phase of lightweight key management protocol

Key agreement phase:For communicating, Data center and substation has to providing authentication one another. Then, the exchanging ofessential parameters takes place among these entities and a session key is established for a secured connection. These steps are explained below:

1st Step, substation generates PG = HF(Certificate‖Isub) and Rq = Isub and transmits to Data center.

Then, after receiving the message, the Data center checks t for message freshness. For substation authentication, estimate PG′ = HF(Certificate‖Isub) which is compared with PG. When both are equal, request of the substation is accepted or else rejected.

Next, Datacenter uses the random number (a, b) for generating the parameter Y= (Gdc*l) + h
To achieve anonymity and private key privacy, both the private keys and random numbers are combined. Then, data center derives m= HF(PG‖Y) and W_1 = HF(Y‖m). Finally, the message undergoes encryption at the data center using symmetric key and then forwarded to the substation. E_G (t, Y, W_1)

2nd Step: Here, substation computes t for message freshness and then estimates m′ = HF(PG‖Y), W_1' = HF(Y‖m) for validating and authenticating Data center. Then,the substation randomly selects u and dand then the

substation generates parameter Zwith private key K = (Gsub*u) + v. Parameter Y undergoes encryption using symmetric key which is then forwarded to the channel.

Following the above steps, substation generates K = HF(PG||Y||Z) and W_2 = H(N||K). The purpose of generating these messages is for validating and authenticating the substation by Data center.

Here, the values estimated are used for generating W'_2. When W_2 and W'_2 are equal, the generated parameter is forwarded by the substation otherwise the connection is dropped out by the Data center. On generating the values, these message which is encrypted using symmetric key E_G = (t, Z, W_2)is transmitted to the Data center.

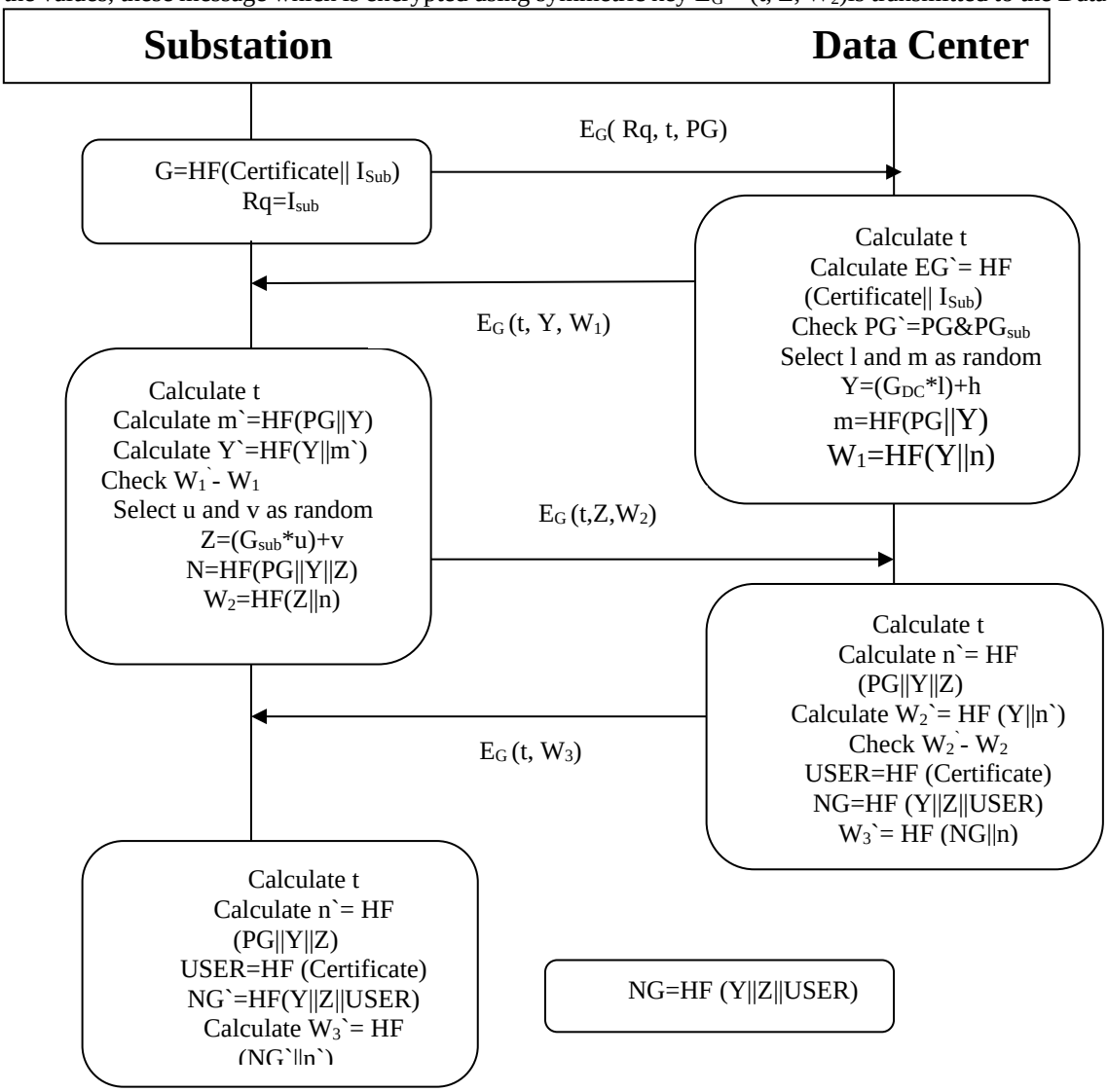

Figure 4:Key agreement phase in light weight key management protocol

Key agreement phase in light weight key management protocol is represented in figure 4 which illustrates the diagrammatic representation of the proposed protocol.

3rd step : Here, Data center tries in generating a session key for secured communication. Once the freshness of message is verified, Data center estimates N′ = HF(PG||Y||Z) and W'_2 = HF(Z||N) for validating and authenticating the substation by comparing W'_2 and W_2.

Once authenticated, U parameter, L3 and session key are generated by theData centeras follows: USER = HF(Certificate), NG = HF(Y||Z||t), W_3 = HF(NG||N) W_3 is used by the substation for the authentication of the Data center. At the end, Data center forwards the message EG (t, W_3) to the substation.

4. Results And Security Analyses

The secured session key and the authentication methodologies are validated by the two entities of the proposed schema. The runtime of the lightweight process and the registration phase's performance evaluation are neglected, because of its lesser weight on the performance of the total system and communication costs. The cost of authentication will be as high as 234.233 ms because block chain cost of queries are 0.225s. Though it is slightly elevated,so it is suitable for smart grid systems applications, because it will have higher resources of computation than our simulation platform.

The proposed schema is implemented for security analysis by testing various kinds of attacks and also estimates the privacy, authentication and private security of exchanging data between two entities. However, a small number of frequent attacks are reviewed with the proposed protocol and observed that it is safe against various attacks and threats.

Below figure 5 shows the comparison of graphical analysis of the proposed and existing methods.

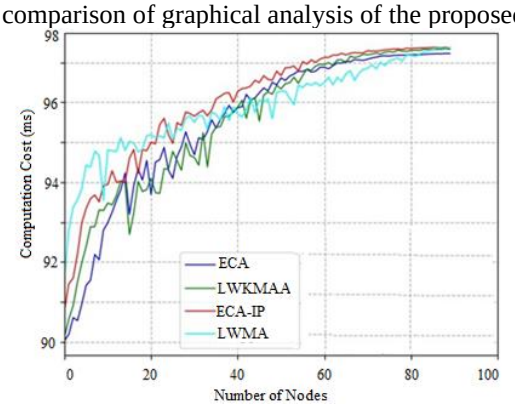

Figure 5: Comparison of communication costs for authentication

Figure 5 interprets that AWKMAA holds good in the comparison of communication among different models with number of nodes

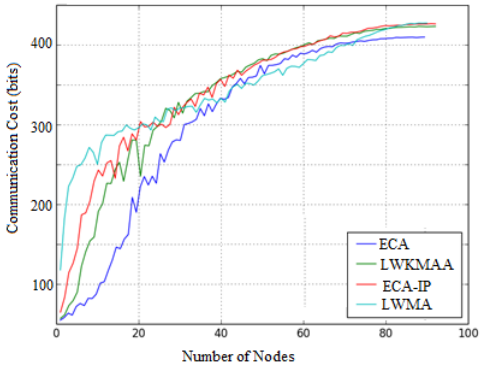

Figure 6: Performance of various authentication and key management techniques for different attacks.

Figure 6 shows the performance of various authentication and key management techniques for different attacks.From the results it is interfered that LWKMAA performance is better as compared to the existing methods.

Table 1: Comparison of different security features

Attacks	**Elliptic curve authentication**	**Light weight message authentication**	**Elliptic curve authentication with Identity authentication**	**Light weight anonymous key distribution authentication**	**Proposed Light weight key management with Autonomous**
Impersonation attack	Passed	Passed	Passed	Passed	Passed
Mutual Authentication	Passed	Passed	Passed	Passed	Passed
Session Key authentication	Passed	Failed	Passed	Passed	Passed
Anonymity	Failed	Passed	Passed	Failed	Passed
Perfect forward secracy	Failed	Failed	Passed	Failed	Passed
Reply attack	Passed	Passed	Passed	Passed	Passed
Man–in–the-middle-attack	Passed	Passed	Passed	Passed	Passed
Safe from DOS attack	Passed	Not discussed	Failed	Not discussed	Passed
No key escrow issue	Not discussed	Not discussed	Failed	Passed	Passed
Private key privacy	Failed	Not discussed	Not discussed	Failed	Passed

5. Conclusion

The ability to provide private and secured communication among end users and AMI is important with infrastructure in smart grids. This paper has introduced a novel anonymous authentication along with key agreement protocol for efficient key management. Some common network attacks were tested with the proposed protocol and was observed that the system was safe against the attacks. This paper provided an optimized protocol with features like reducing communication cost and size of the message providing the solution for overhead issues.

References

1. Yılmaz, Y., & Uludag, S. (2019). Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *Journal of the Franklin Institute*.
2. Maynard, T., & Beecroft, N. (2015). Business Blackout: The Insurance Implications of a Cyber-Attack on the US Power Grid. *Lloyd's of London. Accessed March*, *15*, 2019.
3. Begy, V., Barisits, M., Lassnig, M., & Schikuta, E. (2020). Forecasting network throughput of remote data access in computing grids. *Journal of Computational Science*, *44*, 101158.
4. Foster, I., & Kesselman, C. (Eds.). (2003). *The Grid 2: Blueprint for a new computing infrastructure*. Elsevier.
5. Suleiman, H., Alqassem, I., Diabat, A., Arnautovic, E., & Svetinovic, D. (2015). Integrated smart grid systems security threat model. *Information Systems*, *53*, 147-160.
6. McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, *7*(3), 75-77.
7. Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., ... & Chin, W. H. (2012). Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Communications Surveys & Tutorials*, *15*(1), 21-38.
8. Nicanfar, H., Jokar, P., Beznosov, K., & LEDURng, V. C. (2013). Efficient authentication and key management mechanisms for smart grid communications. *IEEE systems journal*, *8*(2), 629-640.
9. H. Farhangi, "The path of the smart grid," in IEEE Power & Energy Mag., vol. 8, no. 1, pp.18-28, Jan. 2010.
    A. Anzalchi, and A. Sarwat, "A survey on security assessment of metering infrastructure in Smart Grid systems," in Proceedings of the IEEE SoutheastCon 2015, pp. 1-4, Apr. 2015
10. Federal Energy Regulatory Commission. "Assessment of Demand Response and Advanced Metering," Staff Report, Dec. 2014.
11. F.M. Cleveland, "Cyber Security Issues for Advanced Metering Infrasttructure (AMI)," in IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1-5, Jul. 2008
12. Sarkar, S., Chatterjee, S., & Misra, S. (2015). Assessment of the Suitability of Fog Computing in the Context of Internet of Things. *IEEE Transactions on Cloud Computing*, *6*(1), 46-59.
13. Kumar, N., Zeadally, S., & Rodrigues, J. J. (2016). Vehicular delay-tolerant networks for smart grid data management using mobile edge computing. *IEEE Communications Magazine*, *54*(10), 60-66.
14. Wu, L., Wang, J., Choo, K. K. R., & He, D. (2018). Secure key agreement and key protection for mobile device user authentication. *IEEE Transactions on Information Forensics and Security*, *14*(2), 319-330.
15. Kertcher, Z., Venkatraman, R., & Coslor, E. (2020). Pleasingly parallel: Early cross-disciplinary work for innovation diffusion across boundaries in grid computing. *Journal of Business Research*, *116*, 581-594.
16. Silváši, F., & Tomášek, M. (2020). Lean formalization of bounded grids and computable cellular automata defined thereover. *Science of Computer Programming*, *195*, 102471.
17. Alrashed, S. (2020). Key performance indicators for Smart Campus and Microgrid. *Sustainable Cities and Society*, *60*, 102264.
18. Badra, M., & Zeadally, S. (2013, April). Key management solutions in the smart grid environment. In *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)* (pp. 1-7). IEEE.
19. Zhang, K., Lu, R., Liang, X., Qiao, J., & Shen, X. S. (2013, August). PARK: A privacy-preserving aggregation scheme with adaptive key management for smart grid. In *2013 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 236-241). IEEE.
20. Das, S., Ohba, Y., Kanda, M., Famolari, D., & Das, S. K. (2012). A key management framework for AMI networks in smart grid. *IEEE Communications Magazine*, *50*(8), 30-37.
21. Tawde, R., Nivangune, A., & Sankhe, M. (2015, March). Cyber security in smart grid SCADA automation systems. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-5). IEEE.
22. Liu, N., Chen, J., Zhu, L., Zhang, J., & He, Y. (2012). A key management scheme for secure communications of advanced metering infrastructure in smart grid. *IEEE Transactions on Industrial electronics*, *60*(10), 4746-4756.

23. Xia, J., & Wang, Y. (2012). Secure key distribution for the smart grid. *IEEE Transactions on Smart Grid*, *3*(3), 1437-1443.
24. Law, Y. W., Palaniswami, M., Kounga, G., & Lo, A. (2013). WAKE: Key management scheme for wide-area measurement systems in smart grid. *IEEE Communications Magazine*, *51*(1), 34-41.
25. Murugan, S., Jeyalaksshmi, S., Mahalakshmi, B., Suseendran, G., Jabeen, T. N., & Manikandan, R. (2020). Comparison of ACO and PSO algorithm using energy consumption and load balancing in emerging MANET and VANET infrastructure. *Journal of Critical Reviews*, *7*(9), 2020.