On Lightweight Authentication for Smart Grid Network

Vaidehi Dudhwadkar
PG Student
Symbiosis institute of technology, Pune

Himanshu Agarwal
Associate Professor
Symbiosis institute of technology, Pune

Aarti Agarkar
Ph.D Student
Symbiosis institute of technology, Pune

Pratish Ray
B.tech Student
Symbiosis institute of technology, Pune

ABSTRACT

In the last 6-7 years, there is a rapid growth in the development of Smart Grid Network on earth. Smart Grid (SG) is an advancement to the traditional power grid which integrates the power grid with Information and Communication Technology (ICT). SG is a multilayer environment. In this multilayer environment, there are different layers of communications such as Appliance to Home Area Network (HAN), HAN to Building Area Network (BAN) and BAN to Neighbourhood Area Network (NAN). NAN finally connects to Smart Grid Control Center. There are various security challenges at each layer of communication in SG. In this paper, a comprehensive survey of various authentication protocols to address the security threats in SG environment is presented. Study on five different types of authentication protocols such as simple password based, mutual authentication consensus based and password authentication with Juggling is conducted. Simulation study shows that among all protocols, SG-MCPAK and MCEPAK outperforms in terms of number of hashes, passwords, phases, random number and number of packets transferred. Moreover, an improved protocol SG-JMCPAK is suggested, which combines the best of J-PAKE and SG-MCPAK.

Keywords

Smart Grid (SG), Security, Authentication, Elliptic Curve Cryptography(ECC).

1. INTRODUCTION

Information and Communication Technology (ICT) has witnessed a phenomenal growth in the last two decades. With the advances in Internet technology and the rapid development in IEEE communication standards, various devices are now supported by short range smart communication interfaces and are apparently a part of Internet of Things (IoT). At one hand, these new developments in IoT are offering information, communication and remote data storage for intelligent data analytics, on the other hand there is a growing security threat in such wireless interfaces. Smart Grid is one such Utility, which integrates the traditional power grid with Information and Communication Technology, wherein all home appliances are connected to Smart meters and then to smart grid apparently for bidirectional usage of energy and information i.e. from Utility to consumer and from consumer to other consumers for energy trading.

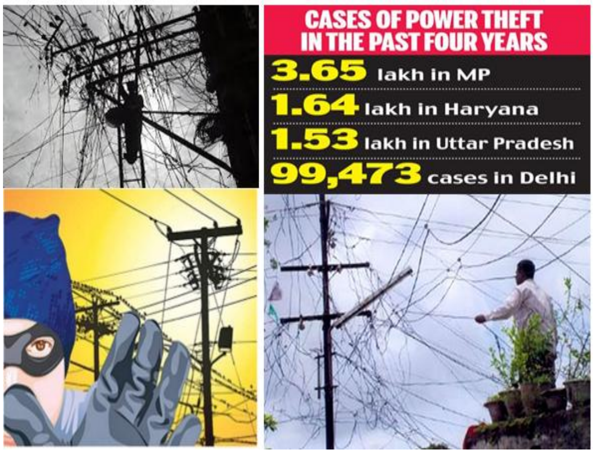
CASES OF POWER THEFT IN THE PAST FOUR YEARS
3.65 lakh in MP
1.64 lakh in Haryana
1.53 lakh in Uttar Pradesh
99,473 cases in Delhi

Fig 1 : Challenges in the existing power grid in India

Recent advances in technology powered by electricity have made the grid resilience increasingly important. For example, the India blackout in July 2012 which had affected more than 350 million people and plunged around 18 states into darkness [17].It has been estimated that utility companies lose more than $25 billion every year due to energy theft around the world. So, it is essential for our traditional electrical grids to evolve into Smart Grids. To enable smooth usage of energy between consumer and producer, one important challenge is preserving the privacy of customers and securing Smart grid network against any cyber attack during information exchange. Hence, implementation of SG without sufficient security measures may cause serious ramification such as uncertainty of grid, utility company fraud, and loss of costumer information and energy-usage data. Furthermore, the complex Advance Metering Infrastructure (AMI) architecture of smart grids, makes it a even challenging to propose refined and robust security operation which can be simply implemented to preserve privacy among the various layers between smart appliances and grid controllers. In this paper, main focus is on privacy challenges in SG, which are mainly based on the protocols used for securing passwords in SG environment.

Contribution in this paper is as below:

- A comprehensive study on various lightweight authentication protocols is conducted, including protocols such as Password Authentication Key Exchange (PAKE),Elliptic curve version of PAKE i.e. EPAKE, Smart Grid Mutual Consensus PAK protocol; SG-MCPAK and Mutual Consensus Elliptic curve PAK; MCEPAK, Password Authentication Key Exchange by Juggling (J-PAKE).

- Analyzed the performance through simulation. The result suggests that SG-MCPAK, MCEPAK and JPAKE protocols offers an improvement with reduced number of hashes, number of packets and number of phases. Among all protocols, SG-MCPAK and MCEPAK outperforms the other protocol in terms of number of hashes, passwords, phases, random number and number of packets transferred.
- Furthermore, an improvement is suggested; SG-JMCPAK which combines the best of J-PAKE and SG-MCPAK.

Organization of the paper is as follows: next section presents a detailed critical review of related research work. Section 3, describes the simulation study of various lightweight authentication protocols followed by security analysis in section 4. Section 5 provides conclusion and future directions.

2. SMART GRID ARCHITECTURE AND OVERVIEW OF AUTHENTICATION PROTOCOLS.

This section presents the architecture of SG and background research work in the area of security challenges in Smart Grid. Fig. 2 shows Smart Grid network, which consists of different communication entities, firstly, various appliances communicate with the smart meter which is considered as Home area network (HAN) and provides the usage information. Building Area Network (BAN) consists of various HANs and communicate the detailing of information to next layer i.e. Neighborhood Area Network (NAN).Finally NAN has communication with Control Center (CC) and usage information is collected at CC. Smart Grid (SG) has bidirectional energy and information flow between the energy user and the utility grid, allowing energy users not only to consume energy, but also to generate the energy and share the excess energy with the utility grid or with other energy consumers. This type of energy user is called the “prosumer”[4].

Energy theft and Power failures are major concerns related to the Power Grid, which lead Smart Grids to replace them [7]. Although this hierarchical network structure is advanced, but this Advanced Metering structure (AMI) extends the attack surface to entire public networks for metering, introducing much vulnerability to cyber attacks [2]. Among all these, providing security and preserving privacy of consumer is the most important challenge in SG [3].

Various solutions have been proposed over the past few years for improving security and privacy issue in SG. It is the wireless media in SG, which is most vulnerable to attacks. Moreover, wireless communication is constrained by limited bandwidth, thus drives further the design philosophy of security protocol to be lightweight in implementation in terms of reducing the overheads in SG communication[1]

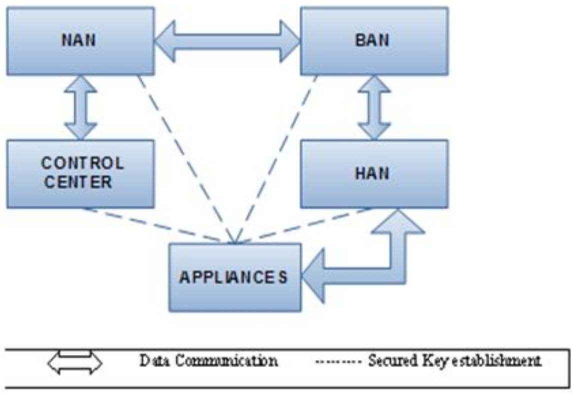

Fig. 2 : Smart Grid Architecture

Although there are many existing Lightweight protocols used, but they have few drawbacks when it comes to reducing communication overheads. Although RSA and AES are highly secured generating strong Random number but, both are time consuming and needs more rounds of communication. Diffie-Hellman is very easy to implement and has good forward secrecy, but is vulnerable to Brute-force attacks. Comparatively, EI-Gamal shows Semantic security and provides Fast signature generation, but has signature verification is expensive. All these crypto-systems have advantages, but are prone to various attacks one of the common attack is Man-in-the-Middle one.EKE and SPEKE can be used to resolve this MITM problem, but are not reliable as partial leaking of password is possible in the exchange process.

Password Authenticated key Exchange (PAKE) protocol provides identity to users and delivers an entity server with Mutual authentication. This design provides security to each user preserving privacy of communication between them [9]. But PAKE is limited to the number of users and uses more hashes to support security. In another attempt, Hasan Nicanfar et al [6, 7] present an extension to the PAKE, called EPAKE and SG-MCEPAK. EPAKE is efficient, secure and resilient to various attacks but it involves complicated group operations and requires pre-computed tables. SG-MCPAK is a multi-layer, consensus based implementation of PAKE which also provides resilience to various attacks but SG-MCEPAK is based on the assumption that all the packets get transferred between all parties without any failure which is bit challenging for wireless sensor network. In PAKE and EPAKE, appliance (A_N) establishes an individual key with each controller following the protocol with each controller, whereas in MCPAKE and MCEPAKE appliance establishes keys using a consensus. This uses less packets and less pre shared passwords for authentication.

Furthermore, as a recent development, Password Authentication Key Exchange by Juggling (J-PAKE) scheme came into use [10].J-PAKE is based on Zero-Knowledge Proof (ZKP) and suggests that the Schnorr’s signature J-PAKE can provide resilient to offline dictionary attacks. Also J-PAKE does not require any Public Key Infrastructure (PKI). On the contrary, J-PAKE is computationally expensive for password authentication purpose.

Based on the critical review in this section, it is suggested that the next lightweight security protocol should advance J-PAKE inheriting consensus approach of MCPAKE. Next section presents a progressive study on various lightweight authentication protocols.

3. AUTHENTICATION PROTOCOLS FOR SMART GRID NETWORK

3.1 Simple Diffie-Hellman

Classical Diffie-Hellman protocol [15] is used to secure any communication channel between two parties using a symmetric key. However the security in the Diffie-Hellman key exchange depends the agreement between the communicating entities which apparently is driven by careful selection of a random number and large prime number used to increase the complexity in the generation. Even after the careful selection of random base (g) and large prime number (p), Diffie-Hellman alone is vulnerable to the Man In The Middle (MITM) attack.

3.2 PAKE Protocol

Password Authenticated Key Exchange (PAKE) [8] is a cryptographic protocol which allows two parties to share knowledge of a password to mutually authenticate each other and establish a shared key, without explicitly revealing the preshared secret, to any other third party. It establishes a symmetric cryptographic key using Diffie-Hellman exchange. It forms four-phase mutual authentication protocol using Diffie-Hellman multiplicative group of integers modulo p & g, R_A & R_B are the random numbers chosen, shares five hash functions H_1-H_5.For example, consider two parties A and B having IDs , ID_A & ID_B each. Both A & B shares messages using hash functions, which is then calculated to obtain key and verified by both A & B to form a mutual authentication derived by password(pw). This four phase applied to SG for authenticating communication at every level of SG is shown in Figure 3.

This protocol needs 5 hash functions and 8 random numbers with 16 phases & four password shared. Thirty packets are transferred between all controllers which is computationally very costly. But this authentication protocol is safe against most of the general attacks. Diffie-Hellman, RSA and ElGamal algorithms provide security against attacks but at expense of large key size. RSA and ElGamal [16] use 1024 and 2048 bits key.

Elliptical Curve Cryptography (ECC) provides the lightweight implementation of classical RSA, ElGamal and Diffie-Hellman. ECC offers same level of security with the reduced key size. Key size of ECC is 160 bits. Security of most of the emerging embedded applications such Smart card is driven by small key size ,therefore ECC based cryptography is seemingly beneficial in terms of faster computation.ECC is based on points on elliptic curve (x,y) over Z_p. The values of Q_A, Q_B and Q_{AB} are points on ECC curve represented using coordinates (x_A,y_A), (x_B,y_B) and (x_{AB},y_{AB}) respectively.

3.3 EPAKE Protocol

EPAK is ECC version of PAKE protocol. Similary like PAKE, it is assumed that both parties have information about ECC parameters set {a,b,p,G,n,h} and the hash function $\widetilde{H}$ and there is a pre-shared password (pw) agreement between A & B. It works very much similar to PAKE, the only difference is it uses Elliptical Curve theory. This helps to reduce the key size and makes it possible to achieve same level of security with smaller key size. Each point on the curve can be represented using x and y coordinates.

The Figure below shows the steps in this protocol:

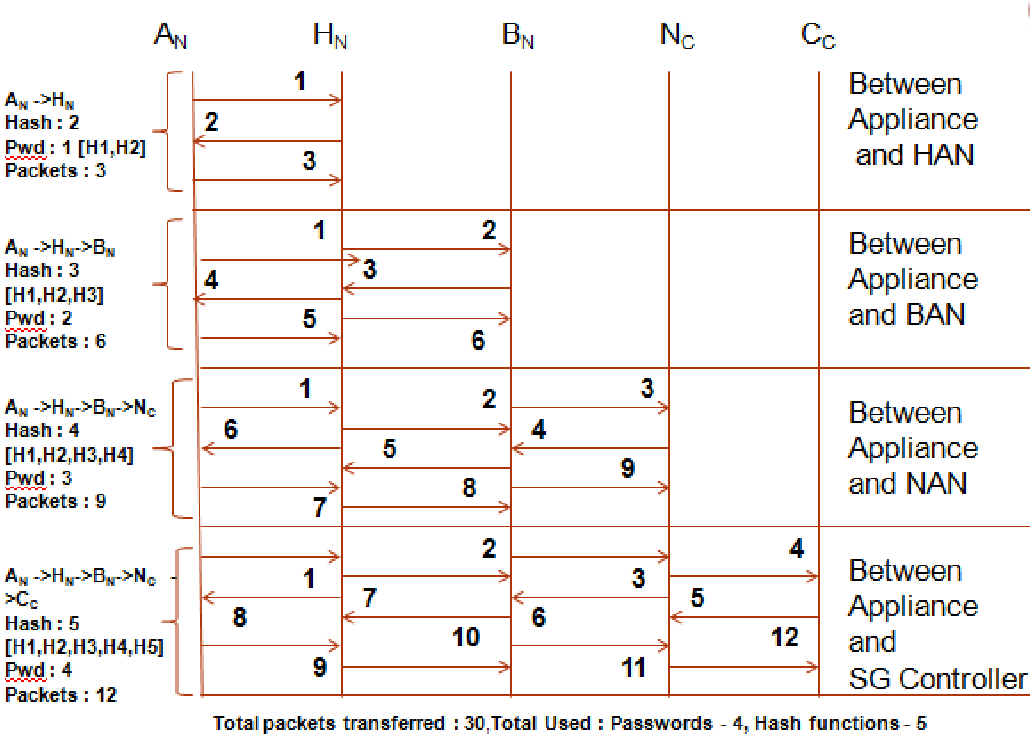

Fig.3: PAKE protocol [8]

Fig. 4 shows that EPAK needs only 1 hash function as compared to PAKE where it, needed 5 hash functions. It uses ECC so it generates shorter and more secure keys. It is even faster in generating the keys than PAKE. Hence, EPAK not only reduces the key size,compared to PAKE but its reliability is much more when it comes to faster mutual authentication.

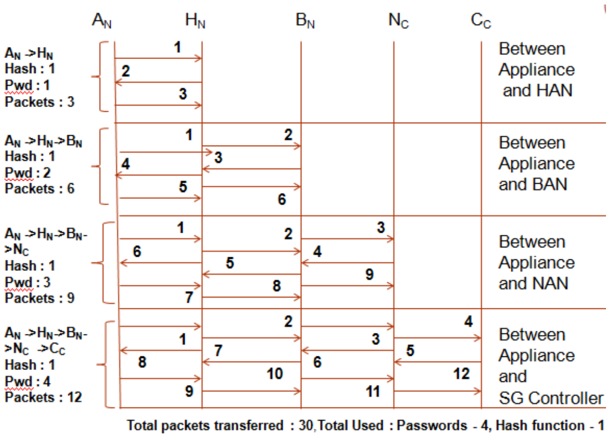
AN HN BN NC CC
AN ->HN
Hash : 1
Pwd : 1
Packets : 3
Between Appliance and HAN
AN ->HN->BN
Hash : 1
Pwd : 2
Packets : 6
Between Appliance and BAN
AN ->HN->BN->NC
Hash : 1
Pwd : 3
Packets : 9
Between Appliance and NAN
AN ->HN->BN->NC ->CC
Hash : 1
Pwd : 4
Packets : 12
Between Appliance and SG Controller
Total packets transferred : 30,Total Used : Passwords - 4, Hash function - 1

Fig.4: EPAKE protocol [6,7]

3.4 SG-MCPAK

SG-MCPAK is Smart Grid Multilayer Consensus Password Authentication key Exchange agreement where it is assumed as a layered based SG architecture with different layers between Appliances A_N, and HAN H_N,BAN B_N,NAN N_C and Smart Grid controller C_C as shown in figure 1.

SG-MCPAK [6] is also a four phase protocol in which initially all parties share the hash function, group based D-H values g and p. Just like PAKE, Appliance and HAN has preshared password pw_{ah}. The controllers H_N, B_N, N_C & C_C have already been authenticated for both the upstream and downstream controllers, and can securely communicate with them. khb, kbn and knc are the symmetric keys which are already shared between H_N B_N, B_N N_C, and N_C C_C respectively. After the execution of four phases, all parties will have their shared keys such as K_{ha}, K_{ba}, K_{nc} and K_{ca}.
The Figure below explains the protocol working: As shown in Fig. 5, SG-MCPAK need only 1 hash function as compared to PAKE where it requires 5 hash functions. Compared to EPAKE it just need one primitive password shared between an appliance and HAN controller to construct four valid individual consensus and authenticated symmetric keys between the appliance and upstream controllers by exchanging only 12 packets instead of 30 in case of EPAKE and PAKE.

3.5 SG-MCEPAK

SG-MCEPAK is ECC based on the extension of SG-MCPAK where ECC is used for defining the values. It works in a similar way as MCPAK.. Hence, follows the same steps for mutual authentication at every–level in SG.

Even though MCPAK and MCEPAK [7] show similar performance analysis. But, compared to MCPAKE, MCEPAKE uses ECC so it generates keys which are shorter in length and secure. As the keys are shorter MCEPAKE generates keys must faster than MCPAKE.

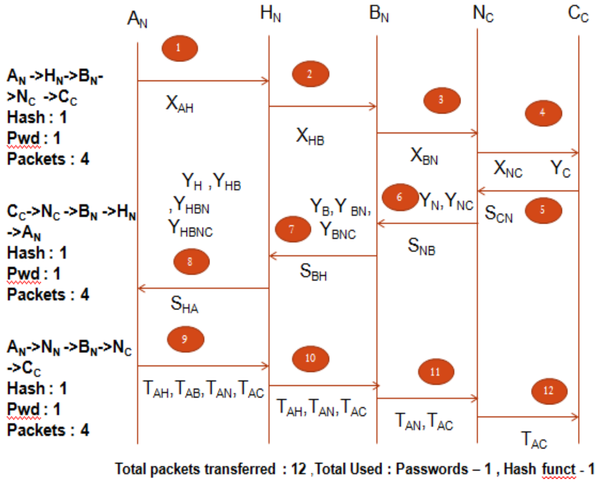

Fig. 5: SG-MCPAK [6]

3.6 J-PAKE

Password-Authentication Key Exchange by Juggling (J-PAKE) is a two-party PAKE protocol. The PAKE research explores an alternative approach to protect passwords without relying on a Public Key Infrastructure (PKI) at all. J-PAKE [11] aims to achieve two goals, Firstly, it allows Zero-Knowledge Proof (ZKP) of the password. One can prove the knowledge of the password without revealing it to the other party. And Secondly, it performs authenticated key exchange. If the password is correct, both parties will be able to establish a common session key that no one else can compute. It has an entirely diverse design approach from all other existing PAKE protocols. It embraces a narrative technique to amend the use of ZKP which makes the overall protocol efficient for practical purpose.

J-PAKE requires four passes of communication between two communicating parties, A and B, but the protocol can be completed in two rounds. There is not any provision for the implicit key confirmation so for having the key confirmation. A and B shares as the secret between them. The secret shared may be a password, or a hash of the password, which actually doesn't make any difference to the protocol. The assumption is made that value of s falls within the range of [1, q-1] and has low-entropy. A selects x_1 & x_2 which belong to [0,q-1] and [1,q-1],while B selects selects x_3 & x_4 which belong to [0,q-1] and [1,q-1].And sends out $g^x{}_1$,$g^x{}_2$ with ZRP for proof of exponents x_1 & x_2.Same happens with B.In second round A & B uses ZRP proof of the exponent x_2s and x_4s.Finally,both parties derive same session.

Fig. 6 shows that, J-PAKE needs 8 phases (2x4) and 20 packets (4x5) to authenticate all the controllers and the appliance as compared to PAKE or EPAKE wherein they need 16 phases and 30 packets in total. J-PAKE shows better and secure results as it excels in Forward secrecy and uses Zero-Proof Knowledge which makes it much more secured in terms of safeness This is more secure than PAKE or EPAKE. It is more efficient to implement JPAKE using Elliptic Curve Cryptography (ECC) in smaller devices.

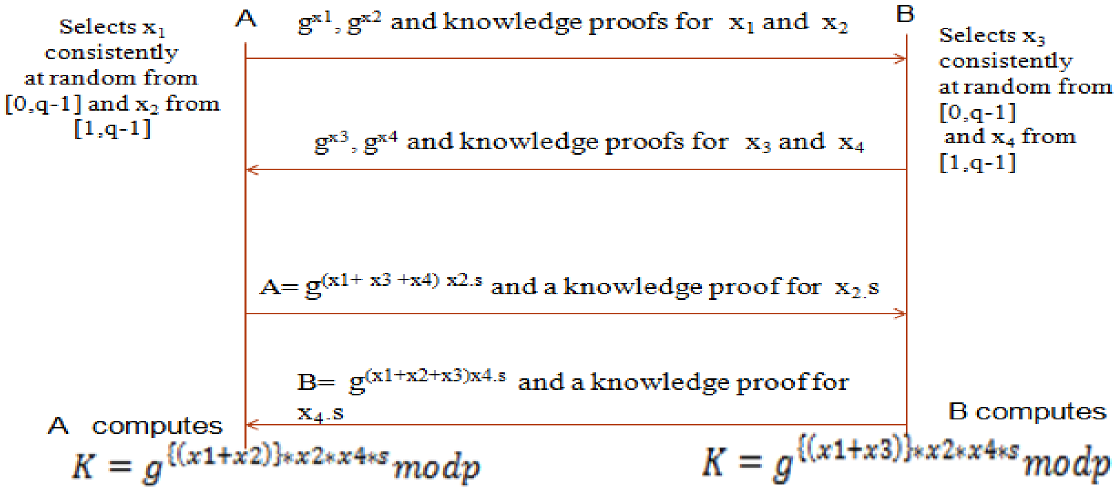
Selects x_1 consistently at random from [0,q-1] and x_2 from [1,q-1]
A
g^{x1}, g^{x2} and knowledge proofs for x_1 and x_2
B
Selects x_3 consistently at random from [0,q-1] and x_4 from [1,q-1]
g^{x3}, g^{x4} and knowledge proofs for x_3 and x_4
A= $g^{(x1+ x3 +x4) x2.s}$ and a knowledge proof for $x_{2.}s$
B= $g^{(x1+x2+x3)x4.s}$ and a knowledge proof for $x_{4.}s$
A computes
$K = g^{\{(x1+x2)\}*x2*x4*s} modp$
B computes
$K = g^{\{(x1+x3)\}*x2*x4*s} modp$

Fig 5: J-PAKE Protocol [10]

3.7 E-JPAKE

In order to address the SG requirements just like EPAKE and ECC version of MCEPAK, ECC version of J-PAKE is presented. J-PAKE uses 256 bit key for encryption, which makes much better for authentication. ECC based J-PAKE works in similar manner compared to J-PAKE. And by applying ECC to it, much better results are being seen. Security is achieved with smaller key size.

For E-JPAKE, it requires 8 phases and 20 packets to authenticate all the controllers and the appliance, just like JPAKE needs only one hash function. ECC based JPAKE provides a small key size, which makes it faster than JPAKE although both incorporate the same level of security.

4. SECURITY ANALYSIS

This section presents the security analysis of various protocols such as PAKE, EPAKE, SG-MCPAK, MCEPAK and J-PAKE protocols using the AVISPA tool [14]. Security analysis has been conducted on the basis of testing these protocols against attacks such as MITM and replay attack and see how safe is the protocol. As shown in Table.1, as compared to PAKE which uses 5 hashes, EPAKE protocol uses only 1 hash function. EPAKE protocol uses ECC to generate a shorter key with a similar level of security. Furthermore, MCPAKE which is based on mutual authentication seems better in terms of reduced number of passwords and phases. As compared to PAKE and EPAKE, MCPAKE uses only 1 hash function, 1 password and only four phases. Whereas, PAKE and EPAKE both use 8 random numbers and 30 packets, MCPAKE offers significant reduction in the number of packets.

Moreover, JPAKE is seemingly better as compared PAKE and EPAKE, JPAKE protocol remains shy as compared to MCPAKE in terms of number of phases and no of packets transferred. In case of JPAKE, it needs 8 phases and 20 packets to authenticate all the controllers and the appliances as compared PAKE, EPAKE wherein needs 16 phases and 30 packets in total. Also JPAKE security is based on Zero-Knowledge-Proof of the password principle; which means one can prove the knowledge of the password without revealing it to any other party. Also J-PAKE protects passwords without relying on Public Key Infrastructure (PKI).The study, concludes that MCPAKE and MCEPAKE protocols incur lower load than PAKE, EPAKE and JPAKE for computations using less number of hash functions and required passwords. Also MCPAKE requires less number of packets transfer to ensure the authentication of passwords. In PAKE, EPAKE and JAPKE appliance (A_N) establishes an individual key with each controller following the protocol with each controller, whereas in MCPAKE and MCEPAKE appliance establishes keys using a consensus. This uses less packets and less pre shared passwords for authentication.

In a single layer scenarios (PAKE, EPAKE and JAPKE), one symmetric key per layer delays the packet travel time as each need to get encrypted and decrypted at each layer (i.e. packets encrypted by B_N should be decrypted by H_N using the key between B_N and H_N, and then encrypted by H_N using the key between H_N and A_N finally gets decrypted by A_N.Whereas in Multilayer scenario (MCPAKE and MCEPAKE), there are shared password between appliance and rest of the controllers, do not need to decrypt and encrypt packets at each layer.

Performance comparison shows that MCPAKE incurs the least load (in terms of number of packets communicated) than PAKE, EPAKE and JPAKE protocols for computations by using less hash functions and required password. On the count of resilience to various attacks, the study revealed that J-PAKE and MCPAKE protocols are most resilient to all types of attacks such as MITM, Replay attack, insider attack and off-line guessing attack.

Furthermore, *an **improved protocol SG-JMCPAK** is suggested which* has the characteristics of JPAKE and can be designed for hierarchical multi-layer architecture of SG using a consensus approach. The information provided in Table revealed that future lightweight protocol design should use a smaller key with minimum number of passes and packets. SG-JMCPAK can support the lightweight security inheriting the best of JPAKE (i.e Zero-Knowledge-Proof) and MCPAK (minimum computational overhead in terms of less packets, minimum phases and hash function). The key can be generated based on four random values generated by all controllers during communication.It will inherit all the advantages of JPAKE and will be resilient to replay attack, MITM attack which are most popular for the smart grid environment.

Proto-col	Hash Function	Pass word	Pha se	Random Number	No of packets
PAKE	5	4	16	8	30
EPAKE	1	4	16	8	30
SG-MCPAK	1	1	4	5	12
MCEPAK	1	1	4	5	12
JPAKE	1	4	8	8	20

Table 1. Comparison of PAKE, EPAKE, SG-MCPAK, MCEPAK and J-PAKE

5. CONCLUSION

In future, the lightweight authentication protocol design is expected to meet the requirements such as minimal key size, less computational overhead and less number of phases in multilayer environment such as Smart Grid. This comprehensive study on various lightweight authentication protocols revealed that JPAKE offers security using Zero-Knowledge-Proof and without involving any public key infrastructure whereas MCPAK protocol provides less overhead. Our work could be extended as follows:

- One possible extension is to investigate how protocols fare based on different types of hash functions. A comparison can be made on the security of the protocols based on the type of hash function used.
- Another possible direction, as suggested in this paper, SG-JMCPAK could be implemented and validated for SG environment to achieve a balance between better security and less computational overhead.

6. REFERENCES

[1] "Introduction to NISTIR 7628 guidelines for smart grid cyber security," National Institute of Standards and Technology (NIST), 2010

[2] Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X. & Zhu, H. Securing smart grid: cyber attacks, countermeasures, and challenges IEEE Communications Magazine, Vol 50, pp 38-45, 2012.

[3] Jiang, Rongxing Lu, Ye Wang, Jun Luo, Chnagxiang Shen,and XueminShen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," *Tsinghua Science and Technology,* Volume 19,Number 2, pp 105-120, April 2014.

[4] A.J Dinusha Rathnayaka,Vidyasagar M.Potdar,Tharam Dillion,Omar Hussain,Samitha Kuruppu,"Analysis of Energy Behavior Profiles by Prosumer,"*IEEE explorer 2012.*

[5] Nicanfar, H.; Jokar, P.; Beznosov, K. & Leung, V. Efficient Authentication and Key Management Mechanisms for Smart Grid , *IEEE Communications Systems Journal,* Vol. 8, pp. 629-640, 2014.

[6] Nicanfar, H. & Leung, V. Smart grid multilayer consensus password authenticated key exchange protocol, *IEEE International Conference on Communications (ICC)*, pp. 6716-6720, 2012.

[7] Nicanfar, H. & Leung, V. Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System Smart Grid, IEEE Transactions on Smart Grid, vol. 4 (1), pp. 253-264, March 2013.

[8] "Password-Authenticated Key Exchange (PAKE) Protocol," International Telecommunication Union (ITU-T), Recommendation X.1035, 2007.

[9] A. H. Koblitz, N. Koblitzb, and A. Menezes, "Elliptic curve cryptography:The serpentine course of a paradigm shift," *Elsevier J. Number Theory,* vol. 131, no. 5, pp. 781–814, May 2011.

[10] F. Hao and P. Ryan, "Password Authenticated Key Exchange by Juggling," *16th Workshop on Security Protocols*, 2008.

[11] D. H. Seo and P. Sweeney, "Simple authenticated key agreement algorithm," *Electron. Lett.*, Vol. 35, no. 13, pp. 1073–1074, Jun. 1999.

[12] S. M. Bellovin and M. Merritt,"EKE: Password-based protocols secure against dictionary attacks," *In Proc. IEEE Computer Society Symposium on Research in Security and Privacy,* Oakland, CA, May 1992.

[13] M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu, and X. Shen, "Towards a light-weight message authentication mechanism tailored for smart grid communications, ‖n *Proc. IFIP SCNC Workshop,* Shanghai, China, Apr. 2011.

[14] AVISPA- Automated Validation of Internet Security Protocols [Online]. Available:http://www.avispa-project.org.

[15] W. Diffie and M. E. Hellman, " New directions in Cryptography" , IEEE Trans. Information Theory, Vol IT-11, pp. 644-654, Nov. 1976.

[16] T. ElGamal, " A public key Cryptosystem and signature scheme based on discrete logarithm", IEEE Trans. Information Theory, Vol IT-31, pp. 469-472, July 1985.

[17] **"**India's largest blackout in History on July 2012", [Online] Avaliable : http://blog.powercuts.in/?p=28.