http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 14 (1): 10-15, 2015
ISSN 1812-5638

REVIEW ARTICLE OPEN ACCESS

DOI: 10.3923/itj.2015.10.15

Authenticated Smart Powercomm: A Review

K. Parkavi Kathirvelu, R. Balasubramanian and Rengarajan Amirtharajan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ARTICLE INFO
Article History:
Received: October 12, 2014
Accepted: February 24, 2015

Corresponding Author:
K. Parkavi Kathirvelu
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT
Smart grid system is a convoluted system in order to provide profound changes in the current grid system. This is fully automated grid utilizes latest information, communication techniques and internet which is truly interconnected and highly open to cyber attacks. Any attack in one location easily propagates through the network and can have immediate impact over wide area network. Without ample security implementation, a smart grid leads to serious outcome such as instability of the grid, malfunctioning of devices, theft in user information and fraud in consumer's energy consumption data. This work briefs the smart grid technologies, key factors, types of attacks and mainly the authentication schemes used to minimize the attacks.

Key words: Smart grid, supervisory control and data acquisition, advanced metering infrastructure, home are network, authentication

INTRODUCTION

As the next decade steps in, it is essential to update the existing grid because conventional grids are unreliable and outdated. The challenges in the existing grid are shown in Fig. 1. In traditional system power production is mainly by fossil fuels which plays major role for green house gas emission that leads to ozone depletion. The antiquated grid slowly response for power quality issues, terror attacks and natural disaster (Fang *et al*., 2011). At present electricity supply consumers are uninformed and having limited opportunities to participate.

Smart grid is smarter and it assimilates information technology, advanced communication and power system. Due to advancement, it increases the efficiency of the system, reduces the electricity cost and improves reliability and power quality (Li *et al*., 2010) .Smart grid not only used to reduce the block outs and brownouts, it also makes the grid greener. Automation and intelligent management improves the efficiency and effectiveness of the power system in the future smart grid. Following benefits turns the smart grid a step forward from the existing grid. (1) Digital, (2) Two way communication, (3) Distributed generation, (4) Network, (5) Sensors throughout, (7) Self healing, (8) Self monitoring, (9) Adaptive and Islanding, (9) Remote check/Test, (10) Pervasive control, (11) Many customer choices, (12) Enabling transition to new energy storage and plug in electric vehicles (Hashmi *et al*., 2011). To make the existing grid smarter the enabling technologies incorporate the following:

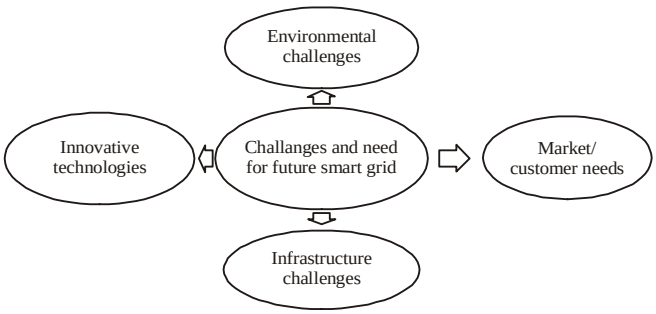

Fig. 1: Challenges and need for future smart transmission grid

- High penetration of renewable energy sources like solar, wind etc… Will mitigate quarrel between human societies and environment sustainability. Development of new materials in power system increases the capability and efficiency
- Advancement in power electronics and power devices will improve the power quality and flexible control in power flow
- Adaptive communication network will allow fast exchange of information and thus increases reliability and system security
- High performance, parallel and distributed computer technologies will enhance real time modeling and simulation of complex power networks
- Transparency, liberty and competition of power market is achieved by mature regulation and policies of power market
- Smart sensors present in the grid increases speed of data transfer and it will provide real time control for the grid (Bari *et al*., 2014; Heirman, 2012; Ipakchi and Albuyeh, 2009; Farhangi, 2010)

Smart grid automation system is layered structure and it includes power plant control, substation control and advanced metering infrastructure. Smart grid utilizes communication technology for monitoring and control of a huge power production, transmission and distribution network without any time lag. For effective power delivery, data exchange is needed between power production unit, RTOs, power consumers and system operators. Smart grid is highly interconnected and open which leads the major security problems (Metke and Ekl, 2010). This study discusses the possibility of cyber attacks in the smart grid and authentication methods used to deal this problem.

KEY COMPONENTS OF SMART GRID

Smart grid known as intellect grid is a four layered structure as shown in Fig. 2 uses bidirectional flow of electricity and communication signals. Advanced Metering Infrastructure (AMI), Supervisory Control and Data Acquisition (SCADA), Communication architecture are the key components of smart grid. Frequently used Acronym in this study and expansion presented in Table 1.

Table 1: Acronym and expansion

RTO	Regional transmission organization
PLC	Programmable logic controller
RTU	Remote terminal unit
AMI	Advanced metering infrastructure
SCADA	Supervisory control and data acquisition system
MTU	Master terminal unit
HMI	Human machine interface
MDMS	Meter data management system
WAN	Wide area network
HAN	Home area network
BAN	Building area network
NAN	Neighborhood area network

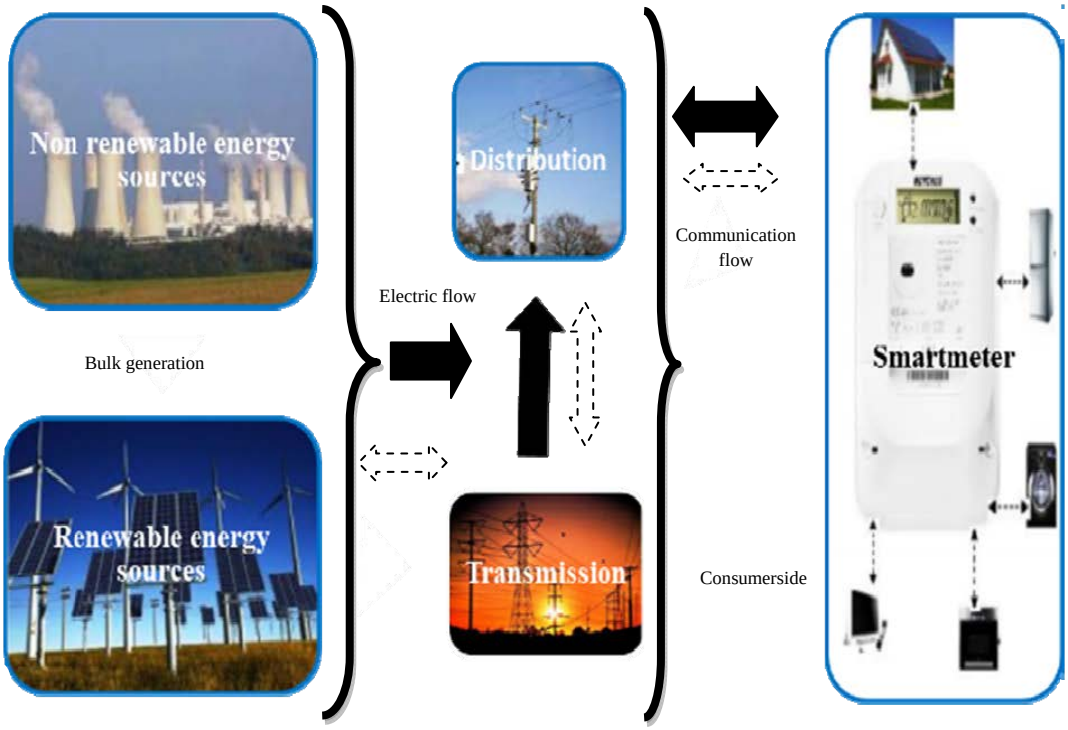

Fig. 2: Layers of smart grid

Supervisory Control and Data Acquisition (SCADA) system: The SCADA is the main block of the substation used for monitor and control of electric power delivery. Master Terminal Unit (MTU), Human Machine Interface (HMI), Remote Terminal Unit (RTU) and Programmable Logic Controller (PLC) are the part of SCADA (Lo and Ansari, 2012).

Advanced Metering Infrastructure (AMI): Smart meter, HAN, Meter Data Management System (MDMS) are put to gather Known as AMI. In today's grid consumers are not getting opportunity to participate in the grid operation. AMI connects consumer and system operator and through this consumer can find out the optimum usage of power and distributer can find out the demand (Depuru *et al*., 2011).

Communication protocols: The IEEE, International electro-technical commission IEC and DNP_3 users group developed the communication standards for smart grid. IEC 60870-5, DNP_3 are the standards used for SCADA, MTU and RTU.

MICROGRIDS

Micro grid is the small scale version of the smart grid. Now a day's environmental awareness resulting from thermal power plant has fortified interest in the development of latest grid technology with renewable energy sources. Micro grids are small independent grid and are separated from grid disturbances or outage. Improved technology products like nano solar cells, nano super capacitors, fuel cells and advancement in power electronic control system will bring more passion about micro grids. Development of micro grid with so many converters development in power electronics (Kathirvelu *et al*., 2014; Balasubramanian *et al*., 2014a, b; Arthishri *et al*., 2014; Kalavalli *et al*., 2013) will make the smart grid pollution free.

Benefaction of communication system in smart grid: Communication occupies major place in the smart grid. It is essential to carry on demand forecasting, self recovery during faults and expedite the consumer about the grid. In smart grid environment communication signals are carried out by using power line, wired line or wireless line depending upon the environment. In power line Communication System (PLC), power lines not only used to transfer power and also used to transmit the data.

Drawback of this method is data signals, cannot propagate through transformers and is applicable between two transformers.

Anatory *et al*. (2013) dedicated wire line cables are used to transmit data in the dedicated wire line communication but this method is comparatively costlier. Wireless communication is broadly used for long distance data transmission because of its high speed and low cost (Yan *et al*., 2012). Communication architecture as shown in Fig. 3 can be broadly classified into three categories: Wide Area Network (WAN), Field Area Network (FAN) and Home Area Network (HAN) (Wang *et al*., 2011).

The devices situated in various geographic areas communicate with each other over WAN. Substation automation, SCADA over IP, recloser controls, relays and capacitor banks are under WAN. NAN devices are placed nearer to each other. Gas meters, electrical meters and load control switches are connected through NAN. The HAN composed of smart in house devices, smart meter and HAN gateway. BAN connects the multiple HAN gateways and communicate with NAN (Fan *et al*., 2013).

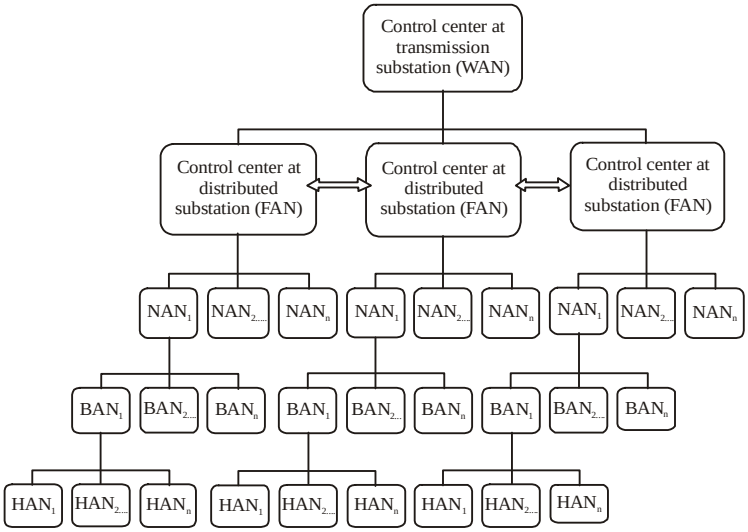

Fig. 3: Communication architecture in smart grid

CYBER ATTACKS AND ATTACKERS

Smart grid is associated with group of many systems and is easily troubled by cyber threats. Natural disaster, disgruntled employees, competitors in the same field, elite hackers and terrorists are the fundamental sources which destroy the structure of the smart grid. Apart from potential benefits human life is invaluable, so it is essential to prevent from attacks Spoofing, Tampering, repudiation, denial of service attack and phishing are some of the influential attacks (Ericsson, 2010; Wei *et al*., 2011; Liu *et al*., 2012).

Spoofing: Spoofing attack is one in which some person or some program masks the original data to get the unlawful advantages. It normally occurs in Wide Area Monitoring (WAMS) system. Phasor Measurement Unit (PMU) plays a major role in WAMS and it receives time stamps from Global Positioning System (GPS). If the hacker forged the time stamps the phase angle measured by a PMU are different and it leads very drastic effect of generator shut down.

Tampering: Energy is nation's property and theft is big crime. Tampering occurs in smart meters and is used to steal the energy. Physical tampering of meter and firmware are the two types of tampering occur in meters.

Denial of service attack (DOS): The DOS attack shut down a network or machine by flooding the target with traffic or crushing services. Smart meter, network devices, communication links and utility business servers are affected by DOS. This affects the control of electricity and stops the power supply.

Repudiation: Authoring information for particular action can be changed by malicious user using this attack. This makes the appeared data to be invalid or misleading.

Phishing attack: Phishing is an attack method used to steel personal information or protected data and also used for identity theft or spreading virus through email.

SMART GRID CYBER SECURITY

Classification of smart grid cyber security: Smart grid security can be categorized into process control security, advanced metering infrastructure security, communication protocol security and power system state estimation security (Metke and Ekl, 2010). Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS) and Industrial Control System (ICS) are subsets of PCS system. Among the three subsets SCADA securities are essential because any malfunctioning of devices produce abundant financial loss and millions of people. Smart meters are connected to consumers directly and are more vulnerable to cyber attacks (Mo *et al*., 2012; Hahn and Govindarasu, 2011; McBride and McGee, 2012). Any attack in the smart meter can lead to false power usage data and in correct billing system instability and financial loss are the main causes for power system state estimation attack. It is essential to protect the communication protocol because smart grid relies many communication protocols to communicate the information between its different components (Bou-Harb *et al*., 2013).

In the modern smart grid millions of consumers are participating in the grids operation, it is troublesome to protect against cyber attack or theft of data. A lot of control and monitoring signals are transmitted every now and then and produce regular traffic in communication network. Any type of interruption due to security issue affects the reliability and efficiency of the system. Privacy, Authentication, Integrity and non repudiation are the foundational security measures that the grid should obey (Iyer, 2011).

Privacy: Privacy indicates that the distributer should be able to send the message to one prescribed consumer privately (Yi *et al*., 2011).

Integrity: The message received by the consumer should reach in correct time without any modification which was sent by the distributer and is used to prevent the theft of information.

Authentication: Authentication indicates that the distributer can be sure of consumer's identity and the data does not come from an imposter. Spoofing attack or forgery can be mitigated using authentication (Vaidya *et al*., 2013).

Non repudiation: Non repudiation denotes that consumer is able to conform that the message came from specific distributer and is used to avoid DOS attack.

Requirement of Authentication in the smart grid: Smart grid is a collective of several systems and subsystems and is easily affected by various attacks that may create innumerable harms to society and the devices in the grid. Data integrity and authentication of users and devices are hit by some attacks like Denial of service, Man in the middle and impersonation. Authentication is used to find the identities of communicating persons to avoid fake access of information. In this work authentication techniques used in two cardinal places of the smart grid such as substation and HAN are focused.

Substation Automation System Authentication (SASA): Control centers in the substations are fully committed with transmission, distribution, maintaining power quality, regulation and inter connection of multiple devices known as intelligent electronic devices IEDs, RTUs and PLCs. It is hard to provide security for Substation Automation System (SAS) because these devices have less memory, restricted processing capability and non standard software platform.

Lu *et al*. (2012) analyzed three different protocols such as RSA, Message Authentication Code (MAC) and One Time Signature (OTS) for SASA. Performance of all three protocols

Table 2: Different authentication schemes and benefits used in HAN

Study	Algorithm used	Benefits
Nicanfar and Leung (2013)	Multilayer consensus based password authentication key exchange elliptic curve cryptography (MCEPAK)	Delay caused by the security process is reduced High security level with a small key size
Kim and Heo (2012)	Matrix based homomorphic hash function	Lowers the amount of computation
Nicanfar and Leung (2012)	Multilayer consensus based password authentication key exchange cryptography (MCPAK)	Reduced system security overhead
Fouda *et al*. (2011)	Diffie Hellman key agreement protocol (DHKAP)	Less memory and communication overhead
Li and Cao (2011) and Nicanfar *et al*. (2011)	Multicast authentication for one time signature	Reduced storage overhead, Signature size is reduced
Nicanfar and Leung (2013)	Enhanced identity based cryptography	Reduced management overhead
Li *et al*. (2014)	Merkle hash tree technique	Less computation complexity and less communication overhead
Xu *et al*. (2008)	A hash tree based authentication technique	Time delay is 10 times lower than RSA

is verified in two different buses Wi-Fi and Ethernet process bus. From this it is concluded that RSA is recommended for smart grid and is not appropriate for delay sensitive messages.

Home area network authentication: Home Area Network (HAN) is used to monitor and control the energy consumed by the customers and to transmit the energy consumption data to utility. Security is major issue because all the consumers are participating directly. In this work numerous authentication techniques given for HAN are analyzed according to their performance.

Nicanfar and Leung (2013) introduced MCEPAK protocol which enables security between home appliances and the various layers of smart gird system. Hash functions are reduced to one in this method and are resilient to several attacks. In this method high level security is provided with less time delay. Nicanfar and Leung (2013) Provided a mutual authentication scheme (Nicanfar *et al*., 2011) Enhanced Identity Based Cryptography (EIBC) and is capable of preventing various attacks with high efficiency. Li *et al*. (2014) Suggested Merkle-Tree based authentication which is having less computation complexity and less communication overhead.

Kim and Heo (2012) developed matrix based homomarphic hash function between smart meter and data management to reduce the computational complexity. Fouda *et al*. (2011) introduced a light weight authentication method based on Diffie-Helman Key Agreement Protocol (DHKAP) and it occupies less memory and communication overhead. Negative of this method is computational time is not analyzed.

One Time Signature (OTS) provide instantaneous authentication without any buffering delay. Biba (Perrig, 2001) and HORSE (Neumann, 2004) are the typical OTS and they have some weakness. In Biba signature size is less but signature time is not limited. HORSE has some limitations when applied to smart grid system. In this method public key size is too large which increases receiver side storage overhead. Liu *et al*. (2012) developed a new tunable signing and verification one time signature (TSVOTS) which reduces the obstacles if Biba and HORSE. Reduced storage overhead and signature size are the benefits of TSVOTS. The available literature different authentication schemes and benefits used in HAN are presented in Table 2.

CONCLUSION

Smart grid produces a new revolution in the present grid. Due to potential benefits of smart grid, this survey explores the key factors of smart grid and the technologies used. SG involves data network transformation and two way communication between consumer and utility. These changes produce new security and reliability challenges for the grid. This survey briefs the threats for SG security mechanisms. Authentication methods are reviewed two different places in SG such as substation automation system and Home area network in which smart meters play vital role. It is no doubt that to make the SG more wide spread it should be free from any security threats and hazards in order to have enhanced future.

REFERENCES

Anatory, J., M.V. Ribeiro, A.M. Tonello and A. Zeddam, 2013. Power-line communications: Smart grid, transmission and propagation. J. Electr. Comput. Eng. 10.1155/2013/948598

Arthishri, K., R. Balasubramanian, P. Kathirvelu, S.P. Simon and R. Amirtharajan, 2014. Maximum power point tracking of photovoltaic generation system using artificial neural network with improved tracking factor. J. Applied Sci., 14: 1858-1864.

Balasubramanian, R., K.P. Karthirvelu, N. Divya, R. Amirtharajan and S. Palani, 2014a. Fuzzy controller based switched boost converter with reduced harmonics for micro grid application. J. Applied Sci., 14: 1928-1935.

Balasubramanian, R., K.P. Kathirvelu, K. Sathishkumar, R. Amirtharajan and S. Palani, 2014b. Fuzzy based single phase double-tuned current source inverter with reduced harmonics for microgrid. J. Applied Sci., 14: 2098-2108.

Bari, A., J. Jiang, W. Saad and A. Jaekel, 2014. Challenges in the smart grid applications: An overview. Int. J. Distrib. Sensor Networks, 10.1155/2014/974682

Bou-Harb, E., C. Fachkha, M. Pourzandi, M. Debbabi and C. Assi, 2013. Communication security for smart grid distribution networks. IEEE Commun. Mag., 51: 42-49.

Depuru, S.S.S.R., L. Wang, V. Devabhaktuni and N. Gudi, 2011. Smart meters for power grid-challenges, issues, advantages and status. Proceedings of the IEEE/PES Power Systems Conference and Exposition, March 20-23, 2011, Phoenix, AZ, USA., pp: 1-7.

Ericsson, G.N., 2010. Cyber security and power system communication-essential parts of a smart grid infrastructure. IEEE Trans. Power Delivery, 25: 1501-1507.

Fan, Z., P. Kulkarni, S. Gormus, C. Efthymiou and G. Kalogridis *et al*., 2013. Smart grid communications: Overview of research challenges, solutions and standardization activities. IEEE Commun. Surv. Tutorials, 15: 21-38.

Fang, X., S. Misra, G. Xue and D. Yang, 2011. Smart grid-the new and improved power grid: A survey. IEEE Commun. Surv. Tutorials, 14: 944-980.

Farhangi, H., 2010. The path of the smart grid. Power Energy Mag., 8: 18-28.

Fouda, M.M., Z.M. Fadlullah, N. Kato, R. Lu and X. Shen, 2011. A lightweight message authentication scheme for smart grid communications. IEEE Trans. Smart Grid, 2: 675-685.

Hahn, A. and M. Govindarasu, 2011. Cyber attack exposure evaluation framework for the smart grid. IEEE Trans. Smart Grid, 2: 835-843.

Hashmi, M., S. Hanninen and K. Maki, 2011. Survey of smart grid concepts, architectures and technological demonstrations worldwide. Proceedings of the IEEE PES Conference on Innovative Smart rid Technologies, October 19-21, 2011, Medellin, Colombia, pp: 1-7.

Heirman, D., 2012. What makes smart grid-smart-and who is in the game? IEEE Electromagn. Compat. Mag., 1: 95-99.

Ipakchi, A. and F. Albuyeh, 2009. Grid of the future. IEEE Power Energy Mag., 7: 52-62.

Iyer, S., 2011. Cyber security for smart grid, cryptography and privacy. Int. J. Digital Multimedia Broadcasting. 10.1155/2011/372020

Kalavalli, C., K. ParkaviKathirvelu and R. Balasubramanian, 2013. Single phase bidirectional PWM converter for microgrid system. Int. J. Eng. Technol., 5: 2436-2441.

Kathirvelu, K.P., R. Balasubramanian, O. Apurna and R. Amritharajan, 2014. Fuzzy logic controller based power conversion system fed from fuel cell. J. Applied Sci., 14: 1736-1742.

Kim, Y.S. and J. Heo, 2012. Device authentication protocol for smart grid systems using homomorphic hash. J. Commun. Networks, 14: 606-613.

Li, F., W. Qiao, H. Sun, H. Wan and J. Wang *et al*., 2010. Smart transmission grid: Vision and framework. IEEE Trans. Smart Grid, 1: 168-177.

Li, H., R. Lu, L. Zhou, B. Yang and X. Shen, 2014. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst. J., 8: 655-663.

Li, Q. and G. Cao, 2011. Multicast authentication in the smart grid with one-time signature. IEEE Trans. Smart Grid, 2: 686-696.

Liu, J., Y. Xiao, S. Li, W. Liang and C.L.P. Chen, 2012. Cyber security and privacy issues in smart grids. IEEE Commun. Surveys Tutorials, 14: 981-997.

Lo, C.H. and N. Ansari, 2012. The progressive smart grid system from both power and communications aspects. IEEE Commun. Surveys Tutorials, 14: 799-821.

Lu, X., W. Wang and J. Ma, 2012. Authentication and integrity in the smart grid: An empirical study in substation automation systems. Int. J. Distrib. Sensor Networks, 10.1155/2012/175262

McBride, A.J. and A.R. McGee, 2012. Assessing smart grid security. Bell Labs Tech. J., 17: 87-104.

Metke, A.R. and R.L. Ekl, 2010. Security technology for smart grid networks. IEEE Trans. Smart Grid, 1: 99-107.

Mo, Y., T.H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, 2012. Cyber-physical security of a smart grid infrastructure. Proc. IEEE, 100: 195-209.

Neumann, W.D., 2004. HORSE: An extension of an r-time signature scheme with fast signing and verification. Proceedings of the International Conference on Information Technology: Coding and Computing, Volume 1, April 5-7, 2004, Las Vegas, NV., USA., pp: 129-134.

Nicanfar, H., P. Jokar and V.C.M. Leung, 2011. Smart grid authentication and key management for unicast and multicast communications. Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies Asia, November 13-16, 2011, Perth, WA, pp: 1-8.

Nicanfar, H. and V.C.M. Leung, 2012. Smart grid multilayer consensus password-authenticated key exchange protocol. Proceedings of the IEEE International Conference on Communications, June 10-15, 2012, Ottawa, ON., pp: 6716-6720.

Nicanfar, H. and V.C.M. Leung, 2013. Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system. IEEE Trans. Smart Grid, 4: 253-264.

Perrig, A., 2001. The BiBa one-time signature and broadcast authentication protocol. Proceedings of the 8th ACM Conference on Computer and Communications Security, November 5-8, 2001, Philadelphia, PA., USA., pp: 28-37.

Vaidya, B., D. Makrakis and H.T. Mouftah, 2013. Authentication and authorization mechanisms for substation automation in smart grid network. IEEE Network, 27: 5-11.

Wang, W., Y. Xu and M. Khanna, 2011. A survey on the communication architectures in smart grid. Comput. Networks, 55: 3604-3629.

Wei, D., Y. Lu, M. Jafari, P.M. Skare and K. Rohde, 2011. Protecting smart grid automation systems against cyberattacks. IEEE Trans. Smart Grid, 2: 782-795.

Xu, K., X. Ma and C. Liu, 2008. A hash tree based authentication scheme in SIP applications. Proceedings of the IEEE International Conference on Communications, May 19-23, 2008, Beijing, China, pp: 1510-1514.

Yan, Y., Y. Qian, H. Sharif and D. Tipper, 2012. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Commun. Surveys Tutorials, 15: 5-20.

Yi, P., A. Iwayemi and C. Zhou, 2011. Building automation networks for smart grids. Int. J. Digital Multimedia Broadcasting. 10.1155/2011/926363