ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Advanced Metering Infrastructure Security Issues and its Solution: A Review

Jing Xu [1], ZhileiYao[2]

Lecturer, School of Information Engineering, Yancheng Institute of Technology, Yancheng Jiangsu, China[1]

Associate Professor, School of Automotive Engineering, Yancheng Institute of Technology, Yancheng Jiangsu, China[2]

ABSTRACT: Advanced metering infrastructure (AMI) is the core component in smart grid. Moreover, two-way communication between the user and the power utility is realized through AMI. Composition of AMI is described. AMI security requirements are illustrated. The threats on the smart meters, communications network, and data collector are analyzed, respectively. Passive and active defenses are investigated. For the passive defense, the traditional encryption technology has low key transportation security, while the public key infrastructure (PKI) used in the whole smart grid has high cost and long computation time and current ID-based authentication mechanism does not offer mutual authentication between smart meter and smart device. When intrusion detection system (IDS) is deployed on AMI key nodes, it is possible to meet the cost effectiveness and computational efficiency and to make up for the passive security policy.

KEYWORDS: Smart grid; advanced metering infrastructure; security and defense policy; public key infrastructure; intrusion detection system

I. Introduction

In the past few decades, the development of power system has not kept pace with industry and society progress. In order to meet the large demand increase on power supply, a vast number of energy resources, including traditional fossil fuels and renewable energy resources, should be managed efficiently. Smart grid is a system that integrates two-way communication technology into the power grid. It can satisfy customer demand on electricity and optimize the resources deployment. It also can ensure safe and reliable power supply. However, power systems are more and more relying on network infrastructures in smart grid and exposing many threats on network security [1]-[2]. Therefore, it is important to develop security mechanisms for smart grid.

Advanced metering infrastructure (AMI) is a key component in smart grid. It can realize two-way communication between customers and electric power company. Its main functions include power measurements, adaptive pricing and user management. It can also provide an interface for other systems [3]-[4].

However, if AMI is not properly used, it will result in grid instability, loss of private information, utility fraud, and unauthorized access to energy consumption data. Therefore, it is vital to ensure the security of AMI [5]-[6].

In this paper, composition of AMI is illustrated in Section II. Security requirements and threats on AMI are analyzed in detail in Sections III and IV, respectively. AMI security solutions, such as passive and active defenses, are provided in Section V. Finally, Section VI concludes the paper.

II. Composition of AMI

Fig. 1 is a structure diagram of AMI. The AMI is comprised of smart meters, data collector, and communications network. AMI transmits the user's electricity consumption information to the meter data management system (MDMS) or other management systems.

A. *Smart meters:*

The smart meter is an advanced electric meter capable of two-way communications with the utility. It serves as a gateway between home area network (HAN) and neighborhood area network (NAN). It measures, records, displays, and transmits data such as energy consumption, generation, text messages, and event logs to authorized systems [8]. It may optionally include a disconnect switch that can be used to remotely provide or disconnect service [8].

DOI: 10.15680/IJIRCCE.2015. 0311001

B. *Communications network:*

AMI communications network achieves a two-way communication between the smart meters and the electrical company's network operations center [5]. AMI includes wide area network (WAN) and NAN, connected by the data collector.

For WAN, it enables communication between the power company's network operations center and data collector. Remote and high-bandwidth communications technologies are adopted, such as WiMAX, cellular (3G, GPRS or CDMA), satellite, and power line communication (PLC).

For NAN, it enables communication between data collector and smart meters. Wireless mesh architecture is used, such as IEEE 802.11, IEEE 802.15 or other private network protocols. It has the characteristics of flexibility, scalability, and low cost.

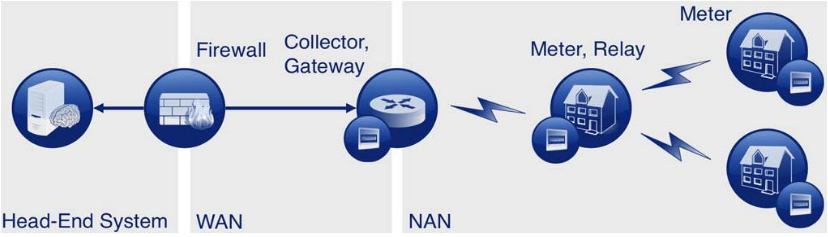

Fig.1.Structure diagram of AMI [7]

C. *Data collector:*

Data collector can collect or receive real-time or periodical data from smart meters [4]. The smart meter data can be transmitted to the power company by the data collector. Similarly, relevant price information and control commands from the power company can be delivered to the user by the data collector.

III. Security Requirements

A. *Confidentiality and Privacy of AMI:*

Confidentiality refers that the information only can be used by authorized users. Any inadvertent or intentional disclosure of relevant data are not allowed. For users in smart grid, they are only allowed to access their own information. For head-end system, only authorized system is allowed to access the data sets. In the smart grid, users do not want their electricity habits and other relevant information gotten by unauthorized persons or company. Therefore, the metering and energy information acquired by smart meter must meet the confidentiality requirements. Confidentiality and privacy is the primary issue in AMI [9].

B. *Integrity of AMI:*

Integrity means that the sensitive data should be neither modified nor deleted in an unauthorized or undetected manner. Power company can obtain the users' data about their consumption and sale electricity, and the customer can get the adapting electricity price information from power company through AMI. The consumption data can help the power company to use energy efficiently. The electricity price helps customers to arrange the use of their electrical appliances in order to reduce the cost. If the hacker tempers the consumption data, the power company may make wrong decision on power generation. In addition, if the customers get the wrong price, they will arrange their electrical appliances according to the false price. It can result in large-scale power outages. Therefore, the integrity of the data is important in AMI.

Power company can also send control command to smart meters. The worst scenario is that the attacker to launch disconnect commands to millions of meters through pretending meter management system. AMI in smart grid requires not only data integrity, but also the integrity of the control command. It is also very important to prevent unauthorized control commands transmitted from AMI system to a smart meter or gateway [10].

C. *Availability of AMI:*

The definition of availability is that authorized users can access to the relevant data at any time. As described above, there are many interactions between the customer and the power company, such as reading value on smart meter, releasing the current tariff, controlling load and distributed generation commands. Therefore, to ensure the availability of information and control commands is critical for smart grid [10].

DOI: 10.15680/IJIRCCE.2015. 0311001

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

IV. THREATS

A. *Smart meters:*

- Privacy.
  Because smart meters send detailed information about how much electricity is being used each time, householder's information and consumption habit can be stolen. From this, the hacker can judge whether the user is at home, and thus achieve his illegal objective. The communication encryption method is often used in the AMI communication, so this type of attack generally includes the following steps: (1) physical access or violent attacks to steal the decryption key; (2) to steal AMI communication information; (3) stealing information by decrypting [11].
- Data tamper.
  The motivation of users to theft energy is to pay less than they used. Theft of service for electric meters often occurs in traditional grid. However, usage data may be tampered after recording or during transmission in smart grid. There is a number of malicious software in the network. Users without a lot of specialized knowledge can achieve tampering the usage data [12].
  Because of the inadequate physical tamper protections, the hackers can interrupt the measurement. Moreover, if the smart meter is physically tampered, the hackers can capture optical port protocol used to communicate with smart meters. If the smart meter is opened, they will put a reader device on this port to capture the other password for other protocols [13]. Without firmware integrity protections in smart meters, meter storage can also be tampered.

B. *Communications network:*

Distributed denial of service (DDoS) is a common attack against availability. The main purpose of DDoS attacks in AMI is to attack data collector, preventing the normal communication between WAN and NAN [4]. Fig. 2 shows DDoS attacks against data collector. Assuming that the attacker's entry point is the smart meter, the detailed attack steps are as follows. Firstly, it can be realized by physical tampering or installing malicious software on the smart meter by using the weaknesses of network, as shown in point 1 in Fig. 2. Secondly, DDoS attacks can be launched in the attacked smart meters, shown in point 2 in Fig. 2. Finally, a large number of malicious network packets are sent to the data collector, given in point 3 in Fig. 2.

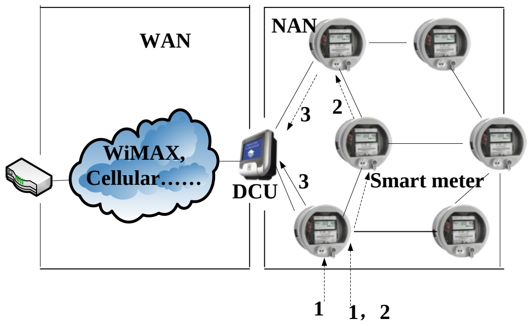

Fig.2.DDoS attacks against data collector

Some of AMI networks are high bandwidth, and the other may be low bandwidth, such as Zigbee, WiFi, and PLC. Therefore, throughput also constraints the security issue. For example, frequently sending large amounts of certificates to the smart meter is not feasible for most AMI network configuration.

In addition, some of the AMI network use public telecommunications services, such as cellular, which is also the security threat factor.

C. *Data collector:*

The remote disconnect function by data collector can be utilized by the attackers to make a large number of outage, as shown in Fig. 3 [4]. The detailed attack steps are as follows. Firstly, it can be realized by physical tampering or installing malicious software on the data collector by using the weaknesses of network or abuse privileges by internal

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

staff, as shown in point 1 in Fig. 3. Secondly, information of smart meters is collected, such as IP address, shown in point 2 in Fig. 3. Finally, a remote disconnect command is sent to target meters, given in point 3 in Fig. 3.

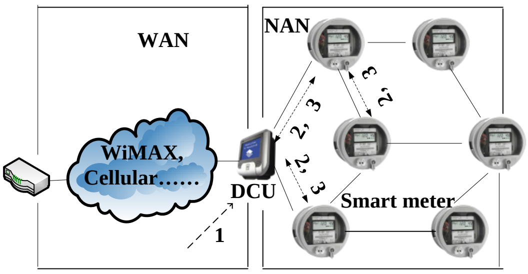

Fig.3.Remote disconnect attack

V. Defense

A. *Passive defense:*

For confidentiality requirements, the physical isolation, anti-eavesdropping, radiation protection, and information encryption are adopted as passive defense. Smart meters are very difficult to physically isolate in smart grid. The information encryption is used to ensure the confidentiality of information [5].

Traditional data encryption technology can prevent the interactive information in smart grid from being stolen and tampered during the public network transmission process. It is a simple and efficient passive security defense, but how to transmit and store keys in the public network is still a serious problem.

When data is bidirectional transmitted in smart grid, confidentiality, integrity, and other security issues exist in a large number of interactive information. The public key infrastructure (PKI) based on smart grid, combining trusted computing to ensure the validity and reliability of the system, was proposed [6]. The certificate is adopted by PKI to manage the public key. The user's public key and other identifying information of users are tied through a trusted third-party certificate authority (CA). The CA is the core of PKI, which manages users’ certificate of PKI. It includes certificate issuance, update, and cancel. Experimental results show that a staff can manage certificates of approximately 1000 users. For example, if an electrical company has 5.5 million smart meters, it will require 5,500 employees to manage these digital certificates [2]. Therefore, manpower and cost are high, and processing cycle is long. In addition, a very high demand on monitoring device is needed to support fast and high-capacity cryptographic computation in smart grid [2].

The PKI is used in many information systems to ensure the security of the system of communication [14]. However, it is difficult to meet the unique requirements of the power grid, such as safe, efficient, real-time operation, scalability, etc.

A security strategy combined PKI with ID authentication was proposed [3]. Fig. 4 shows the PKI based on ID authentication mechanism in smart grid. Certificate authority (CA) is an authentication server in smart grid. All certification of smart devices are stored in the CA list. Meter data management system (MDMS) can grant a certificat to smart meters and user devices. Then smart meters and user devices can achieve mutual authentication through granted cetificates. This method can achieve mutual authentication between the user device and smart meter, which can not be realized by a single ID authentication. It also can reduce a lot of data exchange, which can provide safe and reliable communications environment for smart grid.

B. *Active defense:*

Based on safety requirements on the smart grid, only through a passive defense, such as password protection or encryption technology, cannot solve all security threats. An intrusion detection system (IDS) was introduced into the smart grid preventing the attacks against AMI in smart grid [15] - [18]. Different attacks against AMI are analyzed, which should be timely detected. The information network is divided into three layers, which are HAN, NAN and WAN.

DOI: 10.15680/IJIRCCE.2015. 0311001

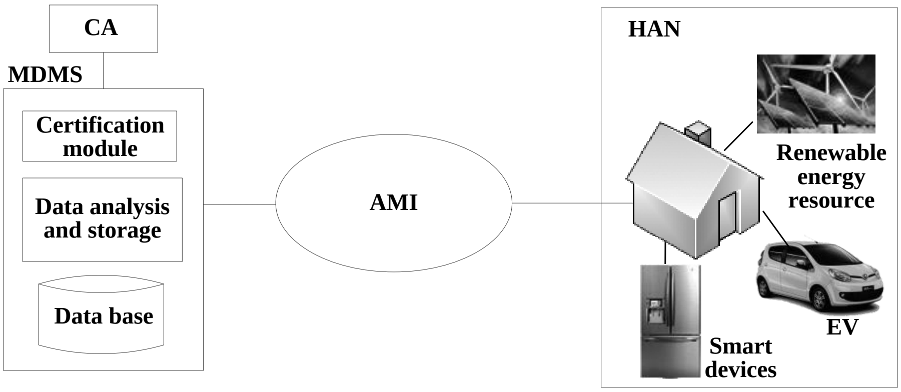

Fig.4.PKI based on ID in smart grid

A HAN-based IDS in smart grid was proposed in [19]. For ZigBee technology, normal behavior in detection library is obtained by extracting some information from the IEEE 802.15.4 standard. All behaviors different from the detection library are considered as invasions. The detection algorithm is based anomaly detection. The detection capability for known attacks is high, but that for unknown attacks is poor.

A NAN-based IDS for in smart grid was proposed in [20]. The system is designed for worm attacks on this layer.

A distributed IDS for the smart grid was proposed in [21]. The IDS is deployed in each layer. Support vector machines (SVM) and artificial immune algorithms are adopted for learning and classifying. Simulation results on KDD'99 dataset show that the security of the system is improved. However, the smart grid has the characteristics of a plurality of nodes, a large amount of data transmission, and high real-time operating requirements. Therefore, the computational efficiency requirement of data collection and classification algorithms is high.

C. *Combined defense:*

Fig. 5 shows a combined security defense policy in smart grid. Encryption, authentication, PKI, access control, and other passive defenses are used to address issues of confidentiality and integrity of the system. The IDS is added into the system to protect the system availability in Fig. 5. However, if the IDS is added to all smart meters, they will be busy to send monitoring information to the control node. It is impossible in a low-bandwidth network. Because the smart meters need lots of memory to store database in order to detect detection when adding the IDS into smart meters, cost of smart meters will be increased. Therefore, IDS can only be deployed in critical nodes.

Fig. 6 gives the structure of the IDS. The IDS is deployed in WAN gateways, data collector and part of smart meters. Compared with the ordinary smart meters, smart meters with IDS need additional storage space and power computing time. In addition, the position of IDS deployment of smart meters should satisfy the following conditions: next to the connection node of data collector and the node that the attacker is difficult to break.

The IDS in the smart meter will monitor all input and output data. If any abnormal data was detected, the IDS will trigger an alarm and record it. Then the IDS in the next level will be informed in order to detect the same detection quickly.

VI. CONCLUSIONS

The AMI security and its solution has been presented in this paper. AMI is comprised of smart meters, data collector, and communications network. The security requirements of AMI are confidentiality, integrity, and availability. The threats on smart meters, data collector, and communications network are analyzed in detail. The solutions for the AMI security are given as follows.

For passive defenses, conventional data encryption technology can prevent interactive information in smart grid to be stolen and tampered during public network transmission. The encryption algorithm is a simple and efficient passive security defense. However, how to transfer and custody the key in public network is still a serious problem. CA is introduced to PKI based on asymmetric encryption algorithm. A trusted and independent third party is chosen to act as a certification center, which is responsible for identifying the true identity of the owner of the public key. As the smart grid is a large and complex system, high manpower, high cost, and long processing cycle exist in the smart grid when only PKI is used.

For active defense, IDS as a proactive preventive method has made a great progress. IDS used in smart grid can monitor real-time network data transmissions and detect intrusion early. It can ensure the safety and reliability of the network. Although it is able to resist attacks on the system largely, high false detection rate, high false positive rate, and speed bottlenecks still exist.

The combined defense can make up for the disadvantages of both passive and active defenses. Therefore, it is a good solution for AMI security.

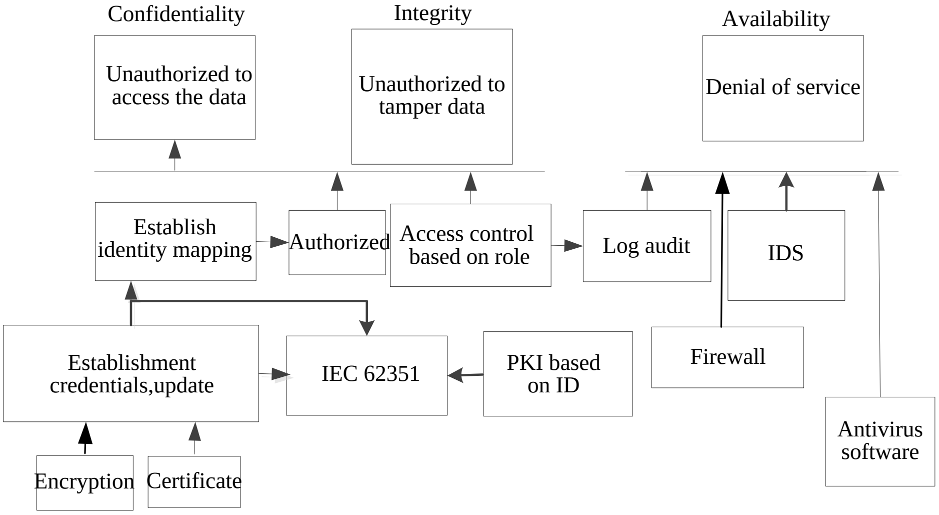

Fig.5.A combined security defense policy

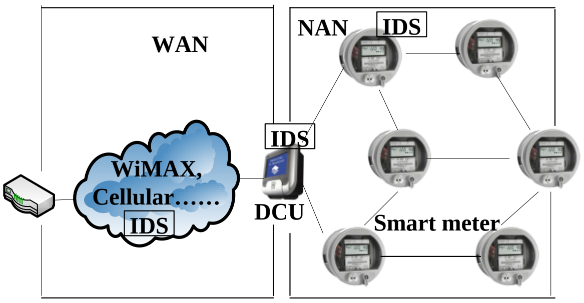

Fig.6.The structure of the IDS

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant 51407153.

References

1. F.Aloul, A. R.Al-Ali, R.Al-Dalky, M.Al-Mardinia, and W.El-Hajjb,‘Smart Grid Security: Threats,Vulenrabilities and Solutions’, International Journal of Smart Grid and Clean Energy, Vol. 1, Issue 1, pp. 1-6, 2012.
2. H.Khurana, M.Hadley, L.Ning, and D. A.Frincke,‘Smart-grid Secutity Issues’, IEEE Security & Privacy, Vol. 8, Issue 1, pp. 81-85, 2010.
3. S.Lee, J.Bong, S.Shin, and Y.Shin,‘A Security Mechanism of Smart Grid AMI Network through Smart Device Mutual Authentication’, IEEE International Conference on Information Networking, pp. 592-595, 2014.
4. D.Grochocki, J. H.Huh, R.Berthier, R.Bobba, W. H.Sanders,A. A. Cardenas, and J. G.Jetcheva,‘AMI Threats, Intrusion Detection Requirements and Deployment Recommendations’, IEEE International Conference on Smart Grid Communication, pp. 395-400, 2012.
5. F. M.Cleveland,‘Cyber security issues for Advanced Metering Infrastructure (AMI)’, IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1-5, 2008.

6. A. R.Meter and R. L.Ekl,‘Security Technology for Smart Grid Networks’, IEEE Transactions on Smart Grid,Vol. 1, Issue 1, pp. 99-107, 2010.
7. Z.Ismail, J.Leneutre, D.Bateman, and L.Chen,‘A Game Theoretical Analysis of Data Confidentiality Attacks on Smart-Grid AMI’, IEEE Journal on Selected Areas in Communications, Vol. 32, Issue 7, pp. 1486-1499, 2014.
8. AMI Security profile V2.0. Web Site [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v2_0.pdf.
9. J.Wang and V. C. M.Leung A survey of technical requirements and consumer application standards for IP-based smart grid AMI network. International Conference on Information Networking, Kuala Lumpur, Malaysia, p.p. 114–119, 2011.
10. M. D. H.Abdullah, Z. M.Hanapi, Z. A.Zukarnain, andM. A.Mohamed,‘Attacks, vulnerabilities and security requirements in smart metering networks’, KSII Transactions on Internet and Information Systems, Vol. 9, Issue 4, pp. 1493-1515, 2015.
11. M. A.Rahman, E.Al-Shaer, and P.Bera,‘A Noninvasive Threat Analyzer for Advanced Metering Infrastructure in Smart Grid’, IEEE Transactions on Smart Grid, Vol. 4, Issue 1, pp. 273-287, 2013.
12. I. A.Tondel, M. G.Jaatun, and M. B.Line,‘Threat modeling of AMI’, 7th International Workshop on Critical Information Infrastructures Security, pp. 264-275, 2012.
13. S.McLaughlin, D.Podkuiko, and P.McDaniel,‘Energy Theft in the Advanced Metering Infrastructure’, 4th International Workshop on Critical Information Infrastructures Security, pp. 1-12, 2009.
14. T.Baumeister,‘Adapting PKI for the Smart Grid’, IEEE International Conference on Smart Grid Communications, pp. 249-254, 2011.
15. E. H.Spafford,‘Intrusion Detection Using Autonomous Agent’, Computer Networks, Vol. 3, Issue 4, pp. 547-570, 2000.
16. J.Kim andP.Bentley,‘Immune Memory and Gene Library Evolution in the Dynamic Clonal Selection Algorithm’, Genetic Programming and Evolvable Machines, Vol. 5, Issue 4, pp. 361-391, 2004.
17. R.Berthier, W. H.Sanders, and H.Khurana,‘Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions’, IEEE International Conference on Smart Grid Communications, pp. 350-355, 2010.
18. N. B.Mohammadi, J.Mišić, V. B.Mišić, and H.Khazaei,‘A Framework for Intrusion Detection System in Advanced Metering Infrastructure’, Security and Communication Networks, Vol. 7, Issue 1, pp. 195-205, 2012.
19. P.Jokar, H.Nicanfar, and V. C. M.Leung,‘Specification-based Intrusion Detection for Home Area Networks in Smart Grids’, IEEE International Conference on Smart Grid Communications, pp. 208-213, 2011.
20. N.Beigi-Mohammadi, J.Misic, H.Khazaei, and V. B.Misic,‘An Intrusion Detection System for Smart Grid Neighborhood Area Network’, IEEE International Conference on Communications, pp. 4125-4130, 2014.
21. Y.Zhang,L. Wang,W. Sun,R. Green, and M.Alam,‘Distributed Intrusion Detection System in a Multi-layer Network Architecture of Smart Grids’, IEEE Transactions on Smart Grid, Vol. 2, Issue 4, pp. 796-808, 2011.

BIOGRAPHY

Jing Xuis a Lecturer in the School of Information Engineering, Yancheng Institute of Technology, Yancheng, China. She received Master of Computer Application (MCA) degree in 2009from Jiangsu University of Science and Technology, Zhenjiang, China. Her research interests are computer networks, smart grid and network safety.

ZhileiYaois anAssociate Professor in the School of AutomotiveEngineering, Yancheng Institute of Technology, Yancheng, China. He received Ph. D. of Power Electronics degree in 2012from Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests are energy technology, renewable Energy.

DOI: 10.15680/IJIRCCE.2015. 0311001